ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y SISTEMAS DE TELECOMUNICACIÓN

PROYECTO FIN DE GRADO

TÍTULO: CIBERCRIMEN Y CIBERTERRORISMO: ¿EXAGERACIÓN MEDIÁTICA O REALIDAD?

AUTOR: JOSÉ LUIS ROCA BLÁZQUEZ

TITULACIÓN: INGENIERÍA TELEMÁTICA

TUTORA: ANA GÓMEZ OLIVA

DEPARTAMENTO: INGENIERÍA Y ARQUITECTURAS TELEMÁTICAS

VºBº

Miembros del Tribunal Calificador:

PRESIDENTE: IGNACIO ANTÓN HERNÁNDEZ

VOCAL: ANA GÓMEZ OLIVA

SECRETARIA: EMILIA PÉREZ BELLEBONI

Fecha de lectura: 28 de marzo de 2014

Calificación:

La Secretaria,

RESUMEN

La expansión de las tecnologías de la información y las comunicaciones (TIC) ha traído muchas ventajas, pero también algunos peligros. Son frecuentes hoy en día las noticias sobre delitos relacionados con las TIC. Se usa a menudo el término cibercrimen y el de ciberterrorismo pero, ¿realmente son una amenaza para la sociedad?

Este trabajo realiza un análisis del cibercrimen y el ciberterrorismo. Para ello se hace un estudio en profundidad desde distintos puntos de vista. En primer lugar se analizan varios aspectos básicos de la materia: el contexto en el que se desarrollan estas actividades, el ciberespacio y sus características, las ventajas que tiene el cibercrimen respecto a la delincuencia tradicional, características y ejemplos de ciberterrorismo y la importancia de la protección de las infraestructuras críticas. Luego se realiza un estudio del mundo del cibercrimen, en el cual se muestran los distintos tipos de cibercriminales, los actos delictivos, herramientas y técnicas más habituales usadas por el cibercrimen, la web profunda y la criptomoneda; se indican asimismo varios de los grupos criminales más conocidos y algunas de sus acciones, y se realiza un estudio de las consecuencias económicas del cibercrimen. Finalmente se hace un repaso a los medios legales que distintos países y organizaciones han establecido para combatir estos hechos delictivos. Para ello se analizan estrategias de seguridad de distinto tipo aprobadas en multitud de países de todo el mundo y los grupos operativos de respuesta (tanto los de tipo policial como los CSIRT/CERT), además de la legislación publicada para poder perseguir el cibercrimen y el ciberterrorismo, con especial atención a la legislación española. De esta manera, tras la lectura de este Proyecto se puede tener una visión global completa del mundo de la ciberdelincuencia y el ciberterrorismo.

ABSTRACT

The expansion of Information and Communications Technology (ITC) has brought many benefits, but also some dangers. It is very usual nowadays to see news about ITC-related crimes. Terms like cyber crime and cyber terrorism are usually used but, are they really a big threat for our society?

This work analyzes cyber crime and cyber terrorism. To achieve it, a deep research under different points of view is made. First, basic aspects of the topic are analyzed: the context where these activities are carried out, cyber space and its features, benefits for cyber criminals with respect to traditional crime, characteristics and relevant examples of cyber terrorism, and importance of critical infrastructures protection. Then, a study about the world of cyber crime is made, analyzing the typology of different kinds of cyber criminals, the most common criminal acts, tools and techniques used by cyber crime, and the deep web and cryptocurrency. Some of the most known criminal groups and their activities are also explored, and the economic consequences of cyber crime are assessed. Finally, there is a review of the legal means used by countries and

organizations to fight against these unlawful acts; this includes the analysis of several types of security strategies approved by countries all around the world, operational response groups (including law enforcement and CSIRT/CERT) and legislation to fight cyber crime and cyber terrorism, with special emphasis on Spanish legal rules. This way, a global, complete view of the world around cyber crime and cyber terrorism can be obtained after reading this work.

ÍNDICE DE CONTENIDOS

CAPÍTULO 1 INTRODUCCIÓN

El ámbito de la seguridad en las comunicaciones y en los sistemas de información cobra una importancia fundamental hoy en día. En los primeros tiempos de la universalización de las redes telemáticas los objetivos eran conseguir unas condiciones de comunicación adecuadas, protocolos comunes y enlaces cada vez más rápidos y eficientes, así como extender el alcance de las redes. En esa época la seguridad no se tomó como consideración imprescindible de diseño, en parte debido a las dificultades para conseguir los citados objetivos básicos. Actualmente esas metas están sobradamente alcanzadas: se da por hecho que las redes llegan a los puntos más remotos del planeta, los enlaces han alcanzado velocidades mucho más elevadas que hace varias décadas y la compatibilidad que ofrece la normalización consigue que dispositivos de distintos fabricantes se comuniquen sin problemas. Con estas condiciones, la sociedad se ha hecho fuertemente dependiente de las tecnologías de la información y las comunicaciones (TIC), lo que conlleva exigencias de seguridad que previamente no se habían tenido en cuenta. La privacidad en las comunicaciones personales se hace

imprescindible y obligatoria según disposiciones oficiales; el secreto de las comunicaciones en los ámbitos gubernamentales y empresariales se convierte en elemento fundamental, y el comercio electrónico mueve muchísimo dinero a diario en todo el mundo. Los ámbitos de la delincuencia y del terrorismo no son ajenos a estas circunstancias y se valen de los medios tecnológicos de comunicación y procesamiento para realizar sus acciones y aprovecharse de los usuarios de cualquier entorno que basan su vida y sus actividades en las TIC.

Con mucha frecuencia aparecen en los medios de comunicación no especializados noticias referidas a acciones ilegales relacionadas con las TIC, en forma de robos, engaños, falsificaciones y otros actos ilícitos. Estos hechos son llamativos por la forma en que se llevan a cabo y por las informaciones que llegan en cuanto a las ganancias o pérdidas que se obtienen con ellos. Sin embargo, es posible que el ciudadano medio, usuario habitual de las nuevas tecnologías, no sea plenamente consciente del tipo y volumen de los delitos que se cometen diariamente y de la posibilidad de que cualquiera pueda ser la víctima en cualquier momento. Además, hay muchas acciones delictivas que no se conocen, por motivos que se comentarán más adelante. La delincuencia relacionada con las TIC constituye un peligro constante y latente, y ha llegado a tener un alcance y una extensión enormes, que implican pérdidas económicas muy elevadas a escala mundial y que exigen una lucha continua por parte de los distintos actores que intervienen.

Este Proyecto pretende realizar un estudio detallado de la situación actual en relación con la delincuencia y el terrorismo en el entorno de las telecomunicaciones y los sistemas de información. Para ello sigue una línea argumental que permite entender la situación en su conjunto incluso a quien no esté implicado y puesto al día en este entorno. A grandes rasgos, se comienza por explicar el contexto en el que se desarrolla el estudio; a continuación se analiza el mundo de la delincuencia y el terrorismo, y por último se estudia el conjunto de acciones que se están llevando a cabo para combatirlo, en forma de respuestas legales. De forma detallada, el contenido de cada capítulo es el siguiente:

El capítulo 2 establece el ámbito en el que se desarrolla el estudio, aportando definiciones básicas que se usarán en el resto del trabajo, resaltando la importancia que tienen las nuevas tecnologías en la sociedad actual, estudiando aspectos particulares que hacen que cometer delitos en entornos TIC sea rentable y a la vez difícil de evitar y perseguir, estableciendo diferencias entre términos relacionados que a veces se confunden (ciberseguridad, ciberdefensa, ciberguerra, ciberataque) y analizando uno de los principales objetivos de los terroristas en estos entornos de las nuevas tecnologías: las infraestructuras críticas. Es conveniente indicar que este Proyecto no tiene como objetivo el estudio del ámbito de la ciberdefensa o la ciberguerra entendidas como conjuntos de políticas y acciones centradas en el ámbito exclusivamente militar.

En el capítulo 3 se realiza un estudio detallado de la delincuencia y el terrorismo en el mundo TIC, describiendo distintos perfiles de delincuentes que se mueven en este ámbito, las acciones ilegales más habituales, las herramientas y técnicas utilizadas,

algunas acciones llevadas a cabo por varios de los grupos más conocidos y, finalmente, las consecuencias económicas de sus actos ilícitos.

El capítulo 4 analiza las respuestas de tipo legal que, en diversos ámbitos nacionales e internacionales, se han establecido para prevenir y combatir los actos de delincuencia y terrorismo que actualmente se están llevando a cabo y que, presumiblemente, se realizarán cada vez con más frecuencia en el futuro. Para ello, se analizan documentos de alto nivel publicados en forma de estrategias de seguridad de distintos ámbitos en multitud de países y en organizaciones supranacionales, prestando especial atención a los publicados en España. A continuación se pasa a un nivel de trabajo más específico y concreto, mencionando distintos grupos de respuesta que, en el ámbito operativo, luchan contra los fenómenos ilegales descritos. Por último, se hace un repaso a distintas disposiciones legales relacionadas con el ámbito del Derecho que pretenden hacer más eficaz la lucha contra la delincuencia y el terrorismo en el entorno de las TIC, con especial énfasis en lo que afecta a las disposiciones penales y procesales españolas.

Este Proyecto pretende cubrir, por lo tanto, distintos aspectos relacionados con la delincuencia y el terrorismo en las nuevas tecnologías, englobándolos desde la perspectiva técnica de bajo nivel hasta la política y estratégica de un nivel más elevado; se ha procurado, por otra parte, que la profundidad de las distintas explicaciones fuera la adecuada, sin entrar en excesivos detalles (por ejemplo, al explicar casos de ataques o de delitos cometidos) pero ahondando lo suficiente en cada uno de los aspectos básicos, técnicos, prácticos, legales y organizativos como para que, al acabar su lectura, pueda tenerse una idea lo más completa posible del estado actual de la temática analizada.

Dada la naturaleza de los temas que han sido objeto de estudio, sobra decir que es imposible que esté completamente actualizado, ya que a diario aparecen noticias nuevas en el ámbito estudiado. Aun así, debe mencionarse que se han tenido en consideración circunstancias e informaciones que estaban saliendo a la luz durante la realización del Proyecto, en la segunda mitad de 2013 y primeros meses de 2014. En lo que se refiere a los apartados dedicados a las técnicas de las acciones delictivas y terroristas, el estudio ha sido exhaustivo y abarca prácticamente todas las que se han llevado a cabo en los últimos años; evidentemente la imaginación de estos actores hará que se inventen nuevas formas de engaño y crimen en el futuro.

Por último, es conveniente mencionar que en la redacción de este texto y para nombrar a los distintos países se ha empleado el nombre recomendado por la Real Academia Española de la Lengua o bien el nombre usual en español según el libro de estilo interinstitucional de la Unión Europea, siguiendo una lista elaborada tras consultas con la Real Academia Española, el Ministerio de Asuntos Exteriores y de Cooperación de España y otras instituciones relacionadas con la toponimia de países extranjeros en idioma español[1].

[1] Véase http://publications.europa.eu/code/es/es-5000500.htm

CAPÍTULO 2 DEFINICIONES Y CONCEPTOS BÁSICOS

Un estudio de la situación actual y de los distintos aspectos relacionados con el cibercrimen y el ciberterrorismo debe empezar sentando unas mínimas bases en cuanto a terminología empleada en este ámbito, pues, aunque algunos términos no tienen una definición concreta y globalmente aceptada, se pueden realizar ciertas aproximaciones para intentar conseguir una visión clara de sus significados. Es importante también, en el entorno del estudio realizado en este Proyecto, destacar la importancia y la dependencia actual que tienen los países desarrollados de las tecnologías de la información y las comunicaciones. Las particularidades de las acciones llevadas a cabo por los grupos del cibercrimen y del ciberterrorismo aumentan enormemente la dificultad de su persecución, y a analizar este aspecto se dedica un punto de este capítulo. Tras analizar con detalle el fenómeno del ciberterrorismo, es conveniente asimismo establecer algunas matizaciones en cuanto al significado de ciertos términos

que a veces se mezclan y se confunden, como ciberseguridad, ciberdefensa y ciberguerra. Finalmente, se dedica la última parte de este capítulo a las infraestructuras críticas, como blancos principales del ciberterrorismo. De esta manera podrá entenderse el resto del trabajo y se hará más comprensible la lectura de textos especializados dedicados a los temas analizados en este Proyecto.

2.1 ALGUNAS DEFINICIONES

Para poder comprender bien la totalidad de lo estudiado en este Proyecto es importante situarse en el entorno en el que se desarrollará este trabajo. Para ello, debe tenerse claro a qué se refiere cada uno de los términos que se emplearán, como ciberespacio, cibercrimen, ciberdelincuencia, ciberterrorismo, ciberataque y otros. Es frecuente que en diversos medios, especializados o no, se usen determinadas expresiones con distinto significado, lo cual a veces puede llegar a alterar el contenido del informe o noticia o incluso la importancia que el lector pueda darle según su propio concepto de cada término. Por ese motivo, y para aclarar qué significado se le da en este trabajo a cada concepto, se facilitarán en este punto diversas definiciones, basadas inicialmente en la etimología de los términos. Posteriormente se ampliará en sucesivos puntos el significado de alguno de ellos y se considerarán diversos aspectos y puntos de vista que pueden matizar las definiciones dadas inicialmente. No se pretende dar definiciones definitivas, pues es difícil poner de acuerdo a todos los implicados en el mundo de la seguridad informática (incluyendo a gobernantes y legisladores). Los límites son a veces difusos en cuanto a cómo se interpretan diversos términos en distintos ámbitos. Es significativo que el *Istituto Affari Internazionali* (Instituto de Asuntos Internacionales[2]) haya editado un documento en septiembre de 2011 titulado "*Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward*" (Definiciones ambiguas en el ciberdominio: costes, riesgos y la forma de avanzar)(1), que destaca que el hecho de no tener definiciones uniformes de ciertas palabras o conceptos en los entornos considerados (Unión Europea y E.E.U.U.) está provocando ineficiencia en la gestión de la seguridad, en la producción normativa y en la aplicación de la ley.

Actualmente hay multitud de términos que comienzan por el elemento compositivo "ciber-", que implica una relación con las redes informáticas(2) según el avance de la vigésima tercera edición del diccionario de la Real Academia Española de la lengua (RAE). Se han formado palabras compuestas anteponiendo dicho prefijo a otras sobradamente conocidas. Una manera sencilla de deducir el alcance de estos términos es trasladar al mundo de las comunicaciones y los sistemas de información el significado del sufijo utilizado, aunque en ocasiones es conveniente particularizar el concepto referido. Así, se habla por ejemplo de cibernauta como persona que navega por

[2] Este Instituto tiene como objetivo "*impulsar el entendimiento de problemas políticos internacionales mediante estudios, investigaciones, reuniones y publicaciones*", según su página web http://www.iai.it

ciberespacios. Precisamente **ciberespacio**[3] es otra de las palabras habitualmente empleadas y que debe ser definida. Habitualmente se entiende que es sinónimo de Internet; sin embargo, conviene matizar esta idea. No todo el ciberespacio es Internet: téngase en cuenta que la propia definición de Internet implica una interconexión de redes privadas y públicas, de tal suerte que todos los equipos son accesibles de alguna manera, ya sea desde cualquier otro equipo conectado a Internet, ya solo desde alguno que se encuentre dentro de la propia red del equipo en cuestión al que se quiera acceder. Al hablar de ciberespacio se puede hacer referencia al complejo y extensísimo conjunto de equipos electrónicos que manejan, transmiten, reciben o procesan información y que se comunican con otros, además de los innumerables elementos de gestión de red que soportan las comunicaciones entre dichos equipos. Se han dado casos de incidentes en redes que no están conectadas a Internet, y que sin embargo se consideran una parte del llamado ciberespacio. Por tanto, no es exacta la correspondencia entre ciberespacio e Internet, siendo el primer término más amplio en su significado, aunque en muchos casos se utilicen como sinónimos.

Se habla también a menudo de **ciberdelito** para hacer referencia a las actividades delictivas o ilegales realizadas valiéndose de los actuales medios y sistemas de información y de comunicación. De acuerdo con la definición dada por el diccionario de la Real Academia Española de la lengua(3)la palabra “delito” tiene varias acepciones:

1. Culpa, quebrantamiento de la ley.

2. Acción o cosa reprobable.

3. Acción u omisión voluntaria o imprudente penada por la ley.

Cualquiera de ellas puede ser considerada en su aplicación a las tecnologías de la información y las comunicaciones. De igual manera, delincuencia es un “conjunto de delitos”, y por tanto se puede usar en los ámbitos adecuados el término “**ciberdelincuencia**”.

También se emplea habitualmente la palabra "**cibercrimen**". Según el mencionado diccionario de la RAE, crimen es la “acción voluntaria de matar o herir gravemente a alguien”. No parece un concepto que pueda trasladarse al mundo de las comunicaciones, pero sí puede utilizarse la primera acepción del citado diccionario, pues de acuerdo con ella, crimen es “delito grave”; también es “acción indebida o reprensible”, y esta acepción puede ser aplicada asimismo al mundo virtual de las comunicaciones y la informática.

De acuerdo con todo lo anterior, parece lógico que puedan emplearse indistintamente los términos ciberdelincuencia y cibercrimen (este último entendido como término general referido al conjunto de acciones delictivas en el ciberespacio); de igual manera,

[3] El término ciberespacio fue empleado por primera vez por William Gibson en su novela “Neuromante” en 1984.

pueden considerarse sinónimas las expresiones cibercrimen (como acción concreta: "se ha cometido un cibercrimen") y ciberdelito.

Otro de los conceptos que se tratarán en este trabajo es el de "**ciberterrorismo**". Según el diccionario de la RAE(4) terrorismo significa "dominación por el terror" y también "sucesión de actos de violencia ejecutados para infundir terror". En este término es conveniente puntualizar el significado cuando se le antepone el prefijo "ciber". En el mundo real el terrorismo está asociado con acciones que provocan daños físicos, habitualmente elevados, que implican destrucción de infraestructuras y a menudo heridas graves o muertes de personas. En el mundo virtual de las TIC parece difícil considerar que alguna acción pueda llevar a tales consecuencias, aunque no es descartable por completo. Sí se puede encontrar, sin embargo, un aspecto en común en ambos entornos, y es la motivación política, religiosa, económica, social o ideológica del terrorista, así como su intención de dar publicidad a sus ideas. Curiosamente se puede adivinar un esfuerzo de adaptación a las nuevas realidades por parte de la RAE, pues la próxima edición del diccionario (vigésimo tercera) aportará una tercera acepción: "Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos". Este nuevo significado, aun no contemplando otros aspectos además del político, es más concreto y puede adaptarse al mundo TIC. En el punto 2.4 de este trabajo se ahondará en el concepto y definiciones del ciberterrorismo, así como su relación con el cibercrimen.

De igual manera que se forman los términos antes definidos, se pueden considerar otros como **ciberataque**, **ciberamenaza** o **ciberguerra**. Sin embargo, a veces se matizan los significados de algunos de estos conceptos o la relación entre ellos; por ejemplo, en la Estrategia de Ciberseguridad de Nueva Zelanda de 2011(5)se hace la siguiente distinción:

> *Ciberataque: intento de debilitar o comprometer la funcionalidad de un sistema informático, acceder a información o intentar realizar un seguimiento de los movimientos online de particulares sin su permiso.*
>
> *Cibercrimen (o crimen informático): cualquier delito donde la tecnología de la información y las comunicaciones 1) se usa como herramienta para cometer una infracción; 2) es el objetivo de una infracción; 3) es un dispositivo de almacenamiento en la comisión de una infracción.*

La Estrategia de Seguridad Nacional española de 2013, que será analizada en el capítulo 4, hace mención de

> *ciberataques, en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo*

En la práctica, muchos ciberdelitos se realizan mediante alguna acción de ciberataque, y de igual manera, un ciberataque se puede clasificar como un caso particular de ciberdelito.

Los significados de **ciberseguridad** y **ciberdefensa**, aunque en un primer momento, y siguiendo con la línea de estudio etimológico seguida en los párrafos anteriores, puedan ser deducidos sin problema, presentan algunos detalles diferenciadores; de igual manera los términos cibercrimen y **ciberguerra** tienen matices que los diferencian, aun siendo a veces difícil establecer la línea divisoria. Curiosamente y no por casualidad, multitud de textos legales, políticas y estrategias nacionales de seguridad y textos similares rehúsan realizar definiciones claras de los términos antes comentados, si bien los emplean abundantemente. Estos conceptos se comentarán en el punto 2.4 de este capítulo.

De todo lo anterior se puede inferir que no siempre está claro el significado concreto y particular de ciertos conceptos utilizados en el ámbito de la seguridad. En cualquier caso, con lo comentado en este punto y lo que se añadirá en el resto de este capítulo se puede tener una idea bastante buena del alcance de cada concepto tratado a lo largo de todo el Proyecto.

2.2 IMPORTANCIA DEL CIBERESPACIO

Hoy en día todos los países civilizados, o en vías de serlo, mantienen una fuerte dependencia de los sistemas de información y comunicaciones. Esta dependencia existe tanto para los ciudadanos en su ámbito personal como en los entornos empresariales y también en los administrativos y oficiales de funcionamiento de los estados. Gran parte de la vida diaria se basa en la conectividad de diversos sistemas y en la disponibilidad de la información. Piénsese por ejemplo en el constante flujo de información entre entidades bancarias y financieras, o en el funcionamiento de los distintos estamentos gubernamentales de las administraciones en sus diferentes niveles (internacionales, estatales, regionales, locales), o en el necesario intercambio de información, por ejemplo en forma de correos electrónicos, entre empresas (incluyendo a las más pequeñas y llegando, por supuesto, a las de ámbito nacional e internacional). Los ciudadanos utilizan cada vez con mayor frecuencia el acceso a distintos servicios disponibles en Internet para realizar gestiones bancarias, para sus relaciones con la administración, para planificar viajes, realizar reservas en hoteles o adquirir billetes de transporte (tanto de carácter personal como en el ámbito de trabajo), e incluso para usos más lúdicos y culturales como por ejemplo en la adquisición de entradas para distintos espectáculos. Las páginas webs de empresas, organismos oficiales y medios de comunicación se han convertido en la principal fuente de información de que se dispone para publicarla por unos o para consultarla por otros. Es evidente, por tanto, que las tecnologías informáticas y de telecomunicaciones son usadas a diario de manera masiva y para asuntos de gran importancia. Como caso especialmente interesante de la relevancia de la dependencia de las TIC se encuentran las llamadas "**infraestructuras críticas**": son aquellas que no solo son importantes, sino que resultan imprescindibles

para la vida diaria de los países. Estas infraestructuras pueden tener sus sistemas de gestión comunicados por algún tipo de red telemática, y emplearán sistemas informáticos de control, lo cual las convierte en parte del ciberespacio. Su importancia las diferencia de otros servicios que simplemente hacen la vida más cómoda y agradable (no es igual no poder sacar una entrada para el teatro por Internet que la imposibilidad de realizar una transacción económica importante vía web). Las infraestructuras críticas serán objeto de un análisis más detallado en el punto 2.6.

Es evidente que el avance en las TIC ha llevado a la dependencia de estas tecnologías, pero también es claro que esto implica un punto débil para las sociedades dependientes. Cualquier problema, provocado o accidental, que afecte a los sistemas utilizados a diario puede ocasionar consecuencias que pueden ir desde la simple molestia temporal para los usuarios de las tecnologías afectadas a la incapacidad para poder llevar a cabo las funciones propias y normales de empresas y organismos oficiales, incluyendo consecuencias económicas e incluso a la paralización casi completa de un país, si se ven afectadas las infraestructuras críticas. Esto se traduce, a su vez, en consecuencias de pérdidas económicas que pueden llegar a ser muy importantes. De ahí que los gobiernos de los países desarrollados hayan aumentado su preocupación por la seguridad en el ciberespacio. Pero ¿qué aspectos de la seguridad son los que deben ser protegidos?

Es conocido que hay distintas características de los recursos que deben ser protegidas. Habitualmente se habla de la **disponibilidad**; como ejemplo, ¿qué ocurriría si durante un tiempo no estuviera disponible la capacidad de consulta de saldos en cuentas bancarias? Se paralizarían multitud de transacciones y eso ocasionaría pérdidas económicas. También se menciona normalmente la **integridad**: es necesario que la información que se transmita o almacene llegue a su destino sin modificaciones ni alteraciones indeseadas. La **confidencialidad** es otro aspecto clave cuando se trata de seguridad, pues gran cantidad de información transmitida o almacenada debe ser accesible solo a aquellos actores que puedan y deban conocerla. También es imprescindible asegurar la **autenticación**, es decir, la seguridad de que los intervinientes en una comunicación son quieres aseguran ser. Todos estos factores son algunos de los que hay que cuidar y proteger, de tal manera que, ante las distintas amenazas que se presentan, sea conveniente asegurar la disponibilidad de los servicios ofrecidos y del ciberespacio y la integridad y confidencialidad de los datos que por él transitan o se almacenan. Hasta hace algunos años esta preocupación correspondía al usuario final (particular o empresa) que quería proteger sus activos y que podía verse amenazado de manera puntual y aislada. Sin embargo, el gran auge que ha experimentado el cibercrimen en los últimos años y las graves consecuencias que supone han hecho que haya pasado a ser preocupación de la esfera de los distintos gobiernos y organismos internacionales. Para hacer frente al cibercrimen y a los ciberataques ha sido necesaria la inclusión de las nuevas ciberamenazas en las respectivas políticas y estrategias de seguridad y defensa de países y organismos supranacionales. A raíz de ello, el siguiente paso ha sido materializar los aspectos de estas directivas en forma de legislación para poder adaptar las leyes existentes a las nuevas formas delictivas. Como medida adicional y necesaria para combatir el cibercrimen y acometer una ciberdefensa efectiva, se han creado

grupos de respuesta, principalmente en el seno de los cuerpos policiales y estructuras militares. Estas respuestas, tanto de nivel estratégico como de tipo táctico, serán analizadas en profundidad para distintos países y organizaciones en el capítulo 4.

El alcance de la ciberseguridad no se limita a los aspectos mencionados de disponibilidad, integridad, confidencialidad y autenticación. Dado que las TIC permiten el correcto, rápido y eficaz funcionamiento de la vida en todo el mundo civilizado, también permiten que se lleven a cabo acciones delictivas y terroristas que hace décadas no serían posibles (o al menos no sería factible realizarlas con tanta facilidad y tanto alcance). El fácil acceso a Internet permite que multitud de delincuentes la utilicen para engañar a usuarios, interceptar o robar información o denegar de manera relativamente fácil distintos servicios, y por supuesto también para comunicarse entre sí para cometer otros delitos y otras actividades ilegales. En el capítulo 3se analizarán con detalle las acciones delictivas que se suelen cometer, así como los grupos más conocidos que las realizan. No obstante, en el siguiente punto se analizan algunos aspectos particulares del cibercrimen en relación a los delitos tradicionales cometidos fuera del ciberespacio.

2.3 ASPECTOS PARTICULARES DEL CIBERCRIMEN Y PROBLEMÁTICA DE SU ESTUDIO

Se ha comentado anteriormente qué es el cibercrimen, y resulta conveniente analizar en este momento cuáles son las características que hacen fácil cometer ciberdelitos y muy difícil prevenirlos o perseguirlos una vez cometidos. Hay aspectos técnicos, otros de tipo social, también los hay de tipo comercial y económico, e incluso de carácter legal que hacen difícil la lucha contra el cibercrimen y los ciberataques.

La propia naturaleza del ciberespacio, como espacio virtual y no real, que carece de fronteras físicas definidas, favorece la acción de los ciberdelincuentes. Es inmediato acceder a algún sistema informático de cualquier otro país, por lejano que sea, en fracciones de segundo. Por tanto, **el concepto de frontera física no se aplica al ciberespacio**, y es aprovechado por los cibercriminales como una gran ventaja. Tal y como se hablará posteriormente en el capítulo 3, son frecuentes los intentos de engaño a través de correo electrónico. Por ejemplo, uno de los casos más conocidos han sido las llamadas “cartas nigerianas”: miles de personas en todo el mundo recibían correos electrónicos en los que se hacía alusión a falsas fortunas de personas africanas que, al morir, no habían dejado descendencia. Para poder disponer de la herencia, los ciberdelincuentes pedían una mínima cantidad de dinero que, supuestamente, iría destinada a desbloquear trámites administrativos o incluso a sobornar a ciertas autoridades implicadas; a cambio, la víctima que colaborara podría conseguir una cantidad elevada de dinero. Este caso ilustra la utilización de un servicio telemático (el correo electrónico) como paso inicial para la comisión de un delito de estafa, de una manera fácil y cómoda para los ciberdelincuentes y con posible impacto en la población de multitud de países.

En la vida real, en el espacio físico que ocupamos, realizar algún tipo de acción delictiva requiere una serie de condiciones que no son necesarias en el ciberespacio. Como primera diferencia se puede considerar la necesidad o no de presencia física en el lugar de la comisión del acto delictivo. Es evidente que la presencia física implica un riesgo que debe ser asumido para cometer un delito físico. Sin embargo, en el ciberespacio no es necesario habitualmente acudir o permanecer en el sitio o sitios que van a ser objeto del ataque (salvo en escasos casos particulares, como por ejemplo cuando se instala alguna infraestructura en cajeros automáticos para posteriormente copiar información de las tarjetas de crédito o débito usadas por clientes, o para visualizar con alguna cámara el PIN de dichas tarjetas y que el propietario introduce para operar). Se puede cometer un ciberdelito robando credenciales de personas aprovechando algún tipo de *malware*[4], o incluso se puede lanzar un ataque de denegación de servicio[5] a redes que se encuentren a miles de kilómetros de distancia. Precisamente esta capacidad de **actuar a mucha distancia** contra personas, organizaciones o sistemas, relacionada con la **falta de necesidad de presencia física**, es otra de las ventajas que los cibercriminales encuentran en el ciberespacio.

Otro de los factores que hacen atractivas las nuevas tecnologías para los ciberdelincuentes, especialmente para realizar ciberataques de distinto tipo, es el **efecto masivo** que pueden tener sus acciones. Mediante la infección con troyanos de cientos de miles de ordenadores, es posible lanzar ataques simultáneos con consecuencias devastadoras. Lo peor de estos casos es que, en la posterior investigación del origen de estos incidentes, es difícil llegar al causante real de los daños: los ataques provienen de miles de equipos infectados de distintos países, cuyos dueños pueden incluso no ser conscientes de que han sido parte de la infraestructura utilizada para llevar a cabo los ataques. Esto conlleva una enorme **dificultad para identificar al autor** real de los ataques y, por tanto, proporciona un **anonimato** atractivo para los cibercriminales. Pero el anonimato también puede provenir de otras circunstancias distintas a las recién comentadas. Al operar en el ciberespacio los sistemas que intervienen en la comunicación suelen estar identificados de forma única. En redes basadas en la familia de protocolos TCP/IP, es la dirección IP la que identifica a cada equipo o dispositivo. Sin embargo, existen técnicas que permiten camuflar y ocultar hasta cierto punto la dirección de algunos equipos. El anonimato puede provenir de la operación detrás de algún dispositivo de red que realiza funciones de traducción de direcciones (NAT, *Network Address Translation*, traducción de direcciones de red), pero también puede estar basado en la operación en alguna de las **redes ocultas** que existen en Internet y que serán objeto de análisis en el punto 3.6. Podría pensarse que para localizar a

[4] *Malware* es una expresión que viene de *malicious software*, software malicioso o maligno. Engloba una amplia variedad de software como virus, troyanos, gusanos, etc. Se analizarán con detalle en el capítulo 3.

[5] Consisten en evitar que un determinado servicio se preste por los servidores correspondientes, por ejemplo enviándoles millones de paquetes en poco tiempo, de manera que los servidores se colapsen; se les conoce de forma genérica como DoS, por *Denial of Service*.

cibercriminales que se ocultan en una red que cursa tráfico a través de un dispositivo que implementa NAT, bastaría con acudir al responsable de la gestión y operación de ese dispositivo para poder identificar el origen real del ciberdelincuente. Sin embargo, algunos países y organizaciones son reacios a colaborar en la investigación de incidentes. Un ejemplo de ello es la llamada RBN (*Russian Business Network*, Red de Negocios Rusa): inicialmente era un proveedor de servicios de Internet que se dedicaba a actividades lícitas, pero no colaboraba en peticiones de investigación; posteriormente pasó a ser una organización cibercriminal que ofrece servicio de almacenamiento o *hosting* para múltiples actividades delictivas (pornografía infantil, almacenamiento de herramientas delictivas, etc.). Este es un caso de proveedor que facilita el cibercrimen y que no ayuda en la investigación de los incidentes (se comentará más sobre RBN en el punto 3.7). Por tanto, pueden unirse varias circunstancias que impiden la investigación de incidentes y la identificación del autor o autores de ciertas acciones, pues los ciberdelincuentes se valen de unas características técnicas (NAT) y/o de unas **dificultades de colaboración internacional**, con implicaciones políticas en algunos casos, para perpetrar delitos con impunidad.

En la dispersión de *malware* y de elementos nocivos por todo el mundo, que se constituyen como herramientas básicas en muchos tipos de ciberdelitos, interviene en no poca medida la **falta de concienciación de seguridad** del usuario medio y la escasez de conocimientos técnicos por parte de los mismos. La llamada "**ingeniería social**" consiste en engañar a usuarios de sistemas informáticos de diversas maneras aprovechando su falta de conocimientos, excesiva confianza o inocencia; de esta manera se consigue información muy valiosa para el delincuente (datos personales de los usuarios, credenciales de accesos, información de terceros, etc.)

Otro problema de tipo legal es la falta de **adecuación de la legislación penal** en distintos países a las nuevas realidades: los códigos penales contemplaban las penas para los delitos tradicionales, pero no para los realizados en los nuevos medios de comunicación. Aparecían entonces situaciones de vacío legal que impedían procesar a los delincuentes. Posteriormente la legislación se ha ido adaptando, aunque sigue habiendo problemas en algunos casos. Estos aspectos legales se analizarán con más detalle en el capítulo 4.

Para cometer delitos en el ciberespacio **no son necesarios grandes conocimientos técnicos** de comunicaciones o de informática. Como ejemplo inmediato considérense por ejemplo los casos de estafa por correo electrónico comentados anteriormente, aunque hay muchos más casos que se comentarán más adelante. Actualmente en Internet **se pueden encontrar fácilmente herramientas para realizar ciberataques** e instrucciones para manejarlas. Estas herramientas son gratuitas en muchos casos, y en otros están a la venta en mercados negros; en su adquisición se puede elegir de cuántos ordenadores infectados por troyanos y preparados para actuar se desea disponer para realizar un ataque masivo desde muchos puntos del planeta, por ejemplo. Incluso se ha llegado a un grado elevado de sofisticación en el diseño de tales herramientas para permitir un control fácil y efectivo de las mismas. Se pueden programar los ataques para que se ejecuten en una determinada fecha y hora, y se puede asimismo programar con qué frecuencia se quieren repetir. El punto 3.4 está dedicado al estudio de algunas de

estas herramientas. Pero aún hay más: si alguien decide llevar a cabo alguna acción delictiva y considera que no tiene los conocimientos adecuados ni puede adquirirlos fácilmente, siempre **se pueden contratar los servicios de ciberdelincuentes**; ya se han acuñado los términos "*cybercrime-as-a-Service*" y "*cybercrime infrastructure-as-a-service*"(6). En el punto 3.7 se mencionan varios grupos delictivos, algunos de los cuales trabajan bajo encargo.

Los casos comentados dejan ver que el ciberespacio es el medio en el que se mueven los cibercriminales para perpetrar sus acciones, y también el objeto mismo de sus delitos en caso de ataques a sistemas, pero también es una herramienta eficaz para permitir la organización de grupos criminales y la preparación de sus actividades delictivas destinadas al mundo físico. Los algoritmos y métodos de **cifrado de las comunicaciones**, pensados con fines lícitos para proteger la intimidad de los ciudadanos, la confidencialidad de las comunicaciones empresariales y gubernamentales, o las transacciones financieras, se utilizan también por los cibercriminales y ciberterroristas para eludir el control de las fuerzas de seguridad. Esto supone una dificultad añadida enorme en las labores de prevención de acciones criminales (tanto en el ciberespacio como fuera de él) y en las de investigación de pruebas. La reacción de ciertos gobiernos occidentales ha sido establecer programas de espionaje de las comunicaciones, excesivos en opinión de unos y necesarios en la de otros.

Sin embargo, el cifrado de la información no es la única dificultad para prevenir y combatir el cibercrimen. Curiosamente, muchas **víctimas del cibercrimen no hacen público que han sido objeto de ataques, fraude, robo de información o acciones similares**. El temor a la pérdida de credibilidad y de buena imagen, con las consecuencias económicas que pueden acarrear, hace que multitud de acciones delictivas no sean conocidas. Esta circunstancia evita poder analizar el modus operandi y las herramientas utilizadas, y facilita a los cibercriminales poder volver a usarlas en el futuro.

Por si no hay ya bastantes factores que hacen atractiva la comisión de delitos en el ciberespacio, hay que añadir alguna más, como la **proliferación de nuevas plataformas** con vulnerabilidades que son objeto de atención de los cibercriminales. Ha sido conocida recientemente una vulnerabilidad del sistema operativo para terminales móviles y tabletas (entre otros dispositivos) Android que existe desde que se publicaron las primeras versiones hace ya varios años(7). Esa vulnerabilidad ha podido permitir instalar en millones de dispositivos móviles cualquier tipo de *malware* que posibilitará, por ejemplo, el robo de credenciales. Este es un ejemplo indicativo de que no siempre se tienen en cuenta los aspectos de seguridad en el diseño de nuevos sistemas, o quizá de que se prefiere realizar nuevos lanzamientos de productos con determinadas imposiciones temporales descuidando otras circunstancias como la seguridad.

De todo lo anteriormente comentado se puede deducir que los cibercriminales tienen muchas razones para valerse de las TIC para cometer sus acciones y sacar rendimiento de diverso tipo, y además puede comprobarse que la evitación de delitos o su posterior persecución presentan grandes dificultades.

2.4 CIBERTERRORISMO

Se comentó anteriormente en el punto 2.1 el significado de ciberterrorismo derivado de la etimología de la palabra, como forma de dominación por el terror o actos de violencia con el objetivo de infundir terror, pero aplicados al ciberespacio. Este concepto suscita alguna controversia respecto a su alcance y significado concreto. No es de extrañar teniendo en cuenta que ni si quiera fuera del ámbito TIC se llega a una definición clara del concepto "terrorismo". Como ejemplo, considérese lo que se cita en el anexo I del acta final de la conferencia diplomática de plenipotenciarios de las Naciones Unidas en la que se preparaba la creación del Tribunal Penal Internacional(8) en 1998:

> *Deplorando que no se haya podido llegar a un acuerdo sobre una definición generalmente aceptable de los crímenes de terrorismo y los crímenes relacionados con drogas (…)*

El Consejo de Europa había redactado en 1977 un tratado titulado "Convenio europeo para la supresión del terrorismo"(9); en 2005 fue complementado con el "Convenio sobre prevención del terrorismo" (10), y en este documento se define "delito terrorista" como cualquiera de los mencionados y definidos en una serie de 11 tratados listados en el apéndice del citado convenio. Estos tratados contemplan casos como secuestros de aviones, actos contra la seguridad aérea, violencia en aeropuertos de aviación civil, actos contra personas protegidas (como embajadores), protección de material nuclear, seguridad en la navegación marítima, colocación de bombas y similares. Puede observarse la naturaleza especialmente violenta de las acciones que se califican como terroristas, y podría pensarse que fuera de estos casos los delitos no se considerarían terroristas, pero tampoco es así.

De lo que no cabe duda es de que el ciberterrorismo, entendido de cualquiera de las maneras que se acaban de ver, es motivo creciente de preocupación internacional. En 2006, uno de los principales temas en la agenda de la reunión de ministros de justicia, de interior y fiscales generales del G8[6] era la cooperación antiterrorista. Según indicó Nurgaliyev, asistente a la reunión y ministro de Interior de Rusia, en la rueda de prensa posterior a la reunión (11) "*los ministros discutieron la necesidad de mejorar las contramedidas para prevenir el terrorismo y actos terroristas en la esfera de la alta tecnología*". En la IV Conferencia Mundial sobre Seguridad celebrada en Bruselas en 2007 se hablaba de lo que podría ser la mayor amenaza terrorista del futuro, y ya se indicaba que "*un gran ataque electrónico requiere mucho tiempo, mucho dinero y mucha inteligencia, pero estas herramientas son cada vez más accesibles para los delincuentes*", y se afirmaba que aunque el riesgo de un ataque de gran nivel era aún bajo, estaba creciendo de manera espectacular(12).

[6] El G8 es un grupo de países con especial peso en la esfera internacional en el terreno económico, político y militar; está formado por Alemania, Canadá, E.E.U.U., Francia, Italia, Japón, Reino Unido y Rusia.

Si fuera del entorno de las nuevas tecnologías y en un documento como el indicado de Naciones Unidas, que emana de un entorno judicial internacional, no existe un consenso claro ni tan siquiera una definición precisa de terrorismo, puede entenderse que en el ámbito de la materia objeto de este Proyecto se encuentren dificultades igualmente. Pueden tenerse en cuenta no obstante distintos aspectos y puntos de vista con objeto de tener una idea del concepto, independientemente de que los límites de las acciones a las cuales puede calificarse como de ciberterroristas estén más o menos definidos y puedan ser objeto de discusión.

Hay autores y organizaciones que opinan que para considerar una acción como ciberterrorista deben producirse daños especialmente elevados, similares a los que produciría alguna acción terrorista fuera del mundo del ciberespacio. El conocido criptógrafo Whitfield Diffie afirma: "*el terrorismo se caracteriza por atacar a gente inocente para asustar a alguna otra persona y conseguir que haga algo. No estoy seguro de que a un ciberataque se le pueda llamar ciberterrorismo, solo porque sea un ciberataque contra las leyes de alguien*". En un documento del Centro de Estudios Internacionales y Estratégicos norteamericano (CSIS, *Center for Strategic and International Studies*) titulado "*Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*" (Análisis de los riesgos del ciberterrorismo, ciberguerra y otras ciberamenazas)(13) se define ciberterrorismo como "*el uso de herramientas informáticas de comunicación en red para inhabilitar infraestructuras críticas nacionales (por ejemplo energía, transporte, operaciones gubernamentales) o para coaccionar o intimidar a un gobierno o a la población civil*". El autor también lo define como "*la intimidación de la empresa civil por el uso de alta tecnología con propósitos políticos, religiosos o ideológicos, acciones que resultan en la anulación o eliminación de información o datos críticos de infraestructuras críticas*"(14). El propio Barry Collin (a quien se le atribuye la invención del término "ciberterrorismo" en 1997) indica(15) algunos hipotéticos pero posibles ejemplos de ciberterrorismo con consecuencias graves en el mundo físico:

- Acceso remoto a los sistemas de control de alguna fábrica de procesado de cereales, cambiando los niveles de enriquecimiento de hierro y provocando enfermedades o muertes de niños que pudieran ingerirlos posteriormente;
- Colocación de varias bombas controladas por ordenador en una ciudad. Cada bomba estaría transmitiendo una secuencia numérica cifrada única y difícilmente previsible, y las demás estarían recibiendo las secuencias. Tan pronto como una bomba dejara de transmitir su secuencia (por haber sido desactivada o anulada, por ejemplo), las demás bombas explotarían;
- Ataque a los sistemas de control de tráfico aéreo para provocar una colisión de aviones;
- Ataque a los sistemas de control de vías en infraestructuras ferroviarias, provocando accidentes de trenes por colisión o por conducirlos a vías muertas, por ejemplo;
- Alteración remota de las fórmulas de distintos medicamentos de manera que provocaran enfermedades o muertes;

- Cambio remoto de la presión en las conducciones de gas, provocando eventualmente un fallo de alguna válvula y posiblemente alguna explosión posterior.

Se observan unos ciertos requisitos para que se pueda calificar de ciberterroristas alguna acción en el entorno de las nuevas tecnologías. De acuerdo con lo anterior, puede considerarse que aún no se ha visto ninguna acción pura de ciberterrorismo que haya causado un grado muy elevado de daño físico o moral en la población de un país, o en las infraestructuras críticas, como se afirma en (13). Sin embargo, las acciones terroristas en el ciberespacio conllevan otra serie de posibilidades no contempladas en lo comentado hasta ahora.

Ya se ha indicó en el punto 2.1 que los fines de los terroristas, tanto los que realizan sus actividades delictivas en el ciberespacio como los que lo hacen fuera de él, suelen tener raíces de tipo social, económico, político, religioso o ideológico. Además de estos condicionantes, se puede considerar que el ciberterrorismo utiliza el ciberespacio tanto como objetivo de sus delitos como también en forma de instrumento o ayuda para la comisión de los mismos.

El primero de los usos del ciberespacio es quizá el que aún no se ha visto materializado a gran escala ni en muchas ocasiones[7]. Es presumible que en cualquier momento pueda producirse, pues otro aspecto propio de las acciones terroristas es la escala o magnitud de sus acciones (recuérdese el caso de las torres gemelas en EEUU en el año 2001), y como se comentó en el punto 2.3 la escala de los ataques en el ciberespacio puede ser tan grande como se quiera imaginar. El ciberespacio permite que se lance algún tipo de ofensiva que pueda afectar a millones de equipos o de ciudadanos de cualquier parte del mundo. Hasta la fecha no se conoce ningún ataque de gran escala cuyo objetivo haya sido un conjunto de equipos informáticos o de medios de transmisión y que haya tenido motivaciones de tipo terrorista (ha habido casos de ataques que han bloqueado países durante algunos días, como ocurrió en Estonia en 2007 y se explicará en la página 133, pero no se ha considerado un ataque terrorista). Además algunos autores consideran que los grupos terroristas prefieren acciones físicas espectaculares antes que acciones cibernéticas, por los efectos inmediatos y directos en el daño causado y la repercusión mediática.

Por el contrario, en cuanto al uso del ciberespacio como herramienta de apoyo de las acciones terroristas tradicionales, los usos concretos son variados y los ejemplos numerosos. Se sabe que distintas organizaciones terroristas utilizan el ciberespacio (más concretamente, Internet) para diferentes objetivos. Por ejemplo, se suelen utilizar sitios web como plataforma de publicidad de sus ideas o acciones físicas y para reivindicación de los atentados cometidos, aumentando la repercusión de tales acciones. Un ejemplo

[7] En 2003 una parte de EEUU tuvo problemas de distribución de energía eléctrica, al parecer debido a la dispersión del gusano “blaster”, y la “brigada Abu-Nafsa” se atribuyó la autoría. No está claro si dicha brigada aprovechó la infección y se la atribuyó o realmente la preparó y materializó a propósito (14) .

es el grupo llamado *As-Sahab* ("la nube"), cuya función es la producción de media[8] para publicitar las ideas y acciones de Al Qaida. Otro grupo similar es el *Global Islamic Media Front* (GIMF, Frente Islámico Global de Media). Este grupo se dedica también a producir material multimedia relacionado de manera más general con la yihad islámica (aunque también tiene relación con Al Qaida), así como a re-codificar y convertir vídeos a distintos formatos y tamaños para su visualización en distintas plataformas, además de publicarlos en diversos sitios web de almacenamiento gratuito y cómodo acceso. El grupo GIMF también facilita herramientas de comunicación cifrada; precisamente ese es otro de los usos de Internet por parte de los grupos terroristas: la comunicación privada entre células terroristas y simpatizantes, con objeto de organizarse y preparar acciones. En http://gimfmedia.com/tech/en/asrar-al-dardashah/ se puede descargar lo que la propia página titula como el "primer programa islámico para mensajería instantánea cifrada". Lógicamente no haría falta ninguna aplicación especial como la que se puede descargar desde la dirección indicada, pues existen técnicas de cifrado que permiten la privacidad en las comunicaciones. En los sistemas de mensajería asíncronos como el correo electrónico puede emplearse la criptografía de clave pública, con sistemas basados en redes de confianza distribuida como por ejemplo PGP o GnuPG, o bien con infraestructuras de clave pública (conocidas como PKI, *Public Key Infrastructures*) basadas en una tercera parte de confianza, aunque esto no suele ser del gusto de los ciberterroristas; en los de mensajería instantánea hay otras posibilidades como OTR (*Off The Record*[9]). Sin embargo, en entornos activistas como el mencionado de la GIMF no se recomienda ninguno de los sistemas comentados, pues existe una elevada desconfianza en cuanto a las aplicaciones desarrolladas por extranjeros, como indican en la página web http://gimfmedia.com/tech/en/asrar-al-mujahideen/ donde se permite la descarga de otra aplicación considerada allí "el primer programa islámico para comunicación segura por la web" (según la página, "se parece a PGP en sus objetivos, pero con nuevas ventajas y claves de alto secreto"). Otra herramienta que se puede descargar de la misma web (http://gimfmedia.com/tech/en/download-mobile-encryption/) es "*Mobile Encryption for Android and Symbian*", que permite el envío y recepción de mensajes SMS entre plataformas móviles con sistemas operativos Android y Symbian, además de poder enviar ficheros cifrados por correo electrónico[10]. En la Figura 2-1 puede verse la página principal de la web mencionada.

Los usos indicados de publicidad de ideas y atentados y de comunicación privada se materializan también en la capacidad de reclutamiento, formación de activistas y células

[8] Según la RAE, "media" con origen en la expresión en inglés "*mass media*" significa "conjunto de los medios de comunicación".

[9] *Off The Record* es una expresión que se utiliza cuando se quiere contar algo, en reuniones o ruedas de prensa, sin que sea grabado. En este caso hace referencia a un nuevo protocolo de mensajería instantánea cifrada, que usa intercambio de claves Diffie-Hellman, cifrado AES y hash SHA-1, proporcionando servicios de autenticación, cifrado y "*perfect forward secrecy*", de manera que aunque se pierdan las claves privadas nadie puede averiguar el contenido de conversaciones anteriores.

[10] La aplicación utiliza librería Bouncy Castle, empleando el algoritmo Twofish con CBC y claves de 192 bits, además de cifrado de curvas elípticas para el intercambio de claves.

remotas gracias a las herramientas comentadas y a otras, como la esteganografía[11]. Fue muy conocido el caso(16) de un ciudadano austriaco interrogado el 16 de mayo de 2011 por la policía en Berlín tras volver de Pakistán. Se le encontró en la ropa interior diverso material de almacenamiento digital. Entre el contenido guardado se encontraba una película pornográfica y una foto. Los investigadores alemanes consiguieron, tras varias semanas de trabajo, romper el cifrado que permitía esconder en esos ficheros una cantidad de material consistente en más de 100 documentos relacionados con preparativos de futuros atentados, manuales de formación en alemán, inglés y árabe y documentos en los que se discutían nuevos objetivos y métodos de ataque. Entre los planes estaba el secuestro de algún crucero con pasajeros, que serían vestidos con trajes naranjas (como los presos de Guantánamo) e irían siendo ejecutados para exigir la liberación de ciertos presos, con el añadido de grabar las ejecuciones.

No sólo se emplea Internet para publicitar ideas o permitir comunicación cifrada entre activistas. Otra de las facilidades que la red ofrece a los terroristas es la obtención de información de posibles objetivos. Dicha información puede consistir en datos concretos sobre la vida de determinadas personas, datos sobre la agenda próxima de personalidades o grupos políticos, gubernamentales, policiales o militares, e incluso sobre localización exacta de blancos. El terreno de la localización de blancos es especialmente útil para las células terroristas. Téngase en cuenta que hace unos años las imágenes obtenidas desde satélites estaban reservadas a gobiernos con posibilidades económicas especialmente altas. Sin embargo, hoy en día está al alcance de cualquier ciudadano acceder a imágenes de muy alta resolución de prácticamente cualquier parte del planeta. Y las imágenes de satélite se complementan de manera espectacular con otras tomadas a pie de calle de la mayor parte de las ciudades importantes del mundo; así, cualquier persona puede, en su ordenador o su teléfono móvil, ver cómo es una determinada calle, fachada de un edificio, etc. como si estuviera allí. De esa manera es bastante fácil preparar atentados con personas que nunca antes hayan estado presentes en el lugar donde se cometerá.

[11] Técnica para ocultar información dentro de algún soporte, de manera que no se aprecie que existen datos ocultos. El caso más conocido y habitual es ocultar información en archivos de media como fotos o vídeos.

Figura 2-1: Página principal de la web del GIMF

Adicionalmente, y como ejemplo de otro de los usos de Internet con fines de apoyo al terrorismo, puede citarse la posibilidad de financiación por distintos medios (17). Es conocido que se ha utilizado habitualmente el llamado sistema *hawala* para transferir dinero entre distintos elementos terroristas, basado en avales (palabra que, por cierto, parece provenir de *hawala*). Este sistema permite la transferencia de dinero entre dos personas distantes usando intermediarios llamados *hawaladars*, sin que medie traslado físico de dinero ni rastros en sistemas informáticos bancarios[12]. Esto ha impedido realizar un seguimiento adecuado por parte de las fuerzas de seguridad en muchas ocasiones. Este sistema se ha empleado desde hace siglos, y aún se sigue utilizando sin necesidad de medios informáticos. Sin embargo, para conseguir mayor celeridad en las comunicaciones entre los intervinientes, se utilizan actualmente medios telemáticos en Internet en las nuevas transferencias; por ejemplo los *hawaladars* usan la mensajería instantánea para informar sobre el estado de las transacciones en curso, siendo igualmente muy difícil el seguimiento policial en este tipo de sistemas de comunicación que no almacenan los mensajes. Este es un caso claro de uso de herramientas modernas de comunicación para complementar sistemas antiguos de trabajo.

Por otra parte, también se emplean los ciberdelitos "tradicionales", no propios del ciberterrorismo, para conseguir financiación. Algunos de los arrestados tras los atentados en los trenes de cercanías en Madrid en marzo de 2004 conseguían dinero a base de fraudes con teléfonos móviles y tarjetas telefónicas. Y por supuesto, aun no siendo una característica exclusiva del ciberterrorismo y sí en general del cibercrimen, los esquemas habituales de consecución de dinero por medios delictivos físicos fuera del

[12] Según (13), Khalid Sheikh Mohamed, uno de los organizadores del atentado del 11 de septiembre de 2001 en E.E.U.U. y ex jefe de operaciones de Al Qaeda, detenido en Pakistán y preso en Guantánamo (Cuba), utilizó el sistema *hawala* con intermediarios en España.

entorno de las nuevas tecnologías (falsificación de documentos, tráfico de drogas, contrabando, tráfico de personas) pueden verse facilitados con la ayuda de herramientas telemáticas de comunicación.

Como ejemplo del uso del ciberespacio y de las nuevas tecnologías puede citarse el tristemente célebre caso de los ataques terroristas ocurridos en Bombay en 2008, que tuvieron como consecuencia 164 muertos(18). Varios grupos previamente organizados atacaron simultáneamente distintos sitios de la capital india (una estación de trenes, varios hoteles, un restaurante y un hospital). Durante los ataques hubo algunos episodios de disparos contra víctimas de manera indiscriminada, así como secuestros en algunos hoteles. Para la preparación de los ataques, los terroristas utilizaron servicios gratuitos de mapas en Internet, lo que les permitió diseñar con detalle sus acciones, teniendo información sobre entradas y salidas de los sitios atacados, así como coordenadas exactas de los mismos, que fueron utilizadas en diversos dispositivos(19). Durante la fase de ejecución, los terroristas utilizaron terminales móviles Blackberry y tarjetas SIM de distintos países, con los cuales se comunicaron con los organizadores de los ataques. Éstos estaban informados de los movimientos de la policía y se los comunicaban a los asaltantes mediante mensajes cortos (SMS). Además, los organizadores utilizaban comunicación mediante voz sobre IP (VoIP). Todo ello contribuyó a hacer muy difícil el seguimiento de las operaciones de los terroristas por parte de las fuerzas policiales. Además, las publicaciones en distintas redes sociales sirvieron a los terroristas para obtener diversa información en tiempo real, como por ejemplo conocer qué efectos se estaban produciendo en el exterior de los edificios ocupados o posibles reacciones, intenciones y posturas oficiales respecto a los acontecimientos. Tanto es así que se dice que las autoridades indias llegaron a pedir que no se diera información a través de las redes sociales e incluso que algunas cadenas de televisión dejaran de cubrir en vivo los acontecimientos.

¿Cuál es la relación entre cibercrimen y ciberterrorismo? Se puede considerar que una acción de ciberterrorismo es un caso particular de cibercrimen, aunque debe contar con algunas peculiaridades como ya se ha comentado: que se encuentre en un nivel superior en cuanto al daño causado, que confluya alguna motivación política, religiosa, social, económica o ideológica en la acción realizada, que pretenda realizar propaganda o reivindicación de algún atentado que se haya producido, que sirva como soporte para la organización de células terroristas o para preparación de acciones… Se puede decir que los actos de ciberterrorismo constituyen actos de ciberdelitos, pero no todos los ciberdelitos pueden englobarse dentro del ciberterrorismo (por ejemplo: un simple robo de credenciales o el uso fraudulento de los datos de una tarjeta de crédito no serían ciberterrorismo, salvo que tengan como fin último perpetrar alguna acción terrorista o ayudar en el reclutamiento de personal, financiación, etc.).

Una vez se han visto los usos que el ciberterrorismo hace de las nuevas tecnologías para materializar sus acciones, usando el ciberespacio como objetivo o bien como medio para sus intenciones, y su relación conceptual con el cibercrimen, surge una pregunta: ¿a

quién corresponde luchar contra el cibercrimen en general y a quién la lucha contra el ciberterrorismo en particular? Se puede trasladar la discusión sobre estas competencias al terreno del terrorismo tradicional. Hasta ahora las fuerzas de seguridad nacionales han sido las que se han encargado de investigar, combatir y detener a los terroristas. Desde hace unos años, están también involucradas en ciertos aspectos de estas tareas las fuerzas militares, con el motivo de atajar desde el origen la capacidad de organización de los terroristas, y para ello se han lanzado ofensivas militares sobradamente conocidas en países de Asia y África. En el terreno de las TIC está ocurriendo algo parecido: ante la masiva actuación de grupos delictivos en el ciberespacio, y en función de cuáles son los objetivos, las motivaciones y el entorno en el que se desarrollan las diversas acciones, pueden ser los organismos policiales o bien los militares los que estén involucrados; interviene aquí la distinción entre los conceptos de ciberseguridad y ciberdefensa, y entre cibercrimen y ciberguerra.

2.5 CIBERSEGURIDAD, CIBERDEFENSA Y CIBERGUERRA

La seguridad, de manera general, presenta muchas vertientes. Puede hablarse de seguridad vial, ciudadana, física, jurídica, laboral, económica, etc. También puede hablarse de seguridad nacional, y este concepto engloba aspectos que afectan al entorno completo de una nación y a su población en conjunto. La seguridad nacional puede estudiarse en función de las amenazas y riesgos que afectan a un determinado país, como pueden ser los conflictos armados, el terrorismo, el crimen organizado, la estabilidad económica, los flujos migratorios ilegales, las ciberamenazas o los desastres naturales sobrevenidos, entre otros. La ciberseguridad, por tanto, puede ser entendida como uno de los múltiples aspectos que debe englobar la seguridad nacional.

La ciberseguridad sin embargo, al igual que otros términos empleados a lo largo de este proyecto, tampoco tiene una definición clara. La recomendación X.1205 de la UIT-T[13](20), aprobada en abril de 2008, define la ciberseguridad como:

> *El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las*

[13] La Unión Internacional de Telecomunicaciones (UIT) es un organismo de la ONU. La UIT-T es la parte de la UIT que publica recomendaciones para estandarizar las telecomunicaciones.

> *propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:*
>
> - *disponibilidad;*
> - *integridad, que puede incluir la autenticidad y el no repudio;*
> - *confidencialidad.*

Pero por otra parte, se puede encontrar en un documento posterior de la propia UIT relativo a información sobre antecedentes para la Conferencia Mundial de Telecomunicaciones Internacionales de 2012(21) lo siguiente:

> *Sin embargo, aún no existe una definición de ciberseguridad aceptada en todo el mundo y ello obstaculiza los esfuerzos de protección que deben emprenderse a nivel nacional e internacional teniendo presente el carácter transfronterizo que tienen hoy en día las redes y sistemas informáticos.*

Ante esta situación parece difícil disponer de un marco común y adecuado para el estudio de esta disciplina y de cualquier otra asociada a ella, pero, igual que se ha hecho en las páginas anteriores con el concepto de ciberterrorismo, pueden darse algunas pautas para acotar el concepto y el alcance de su estudio.

Ya se comentó en el punto 2.1 que la ciberdelincuencia o cibercrimen engloban una serie de actividades ilícitas que se llevan a cabo utilizando el ciberespacio como herramienta o como objetivo. También se ha señalado en el punto 2.4 que el ciberterrorismo se puede considerar un tipo particular de cibercrimen que cumple con ciertas peculiaridades. En general, los ciberdelitos se llevan a cabo mediante acciones de diversa naturaleza (engaño, utilizando la llamada ingeniería social, infección de sistemas informáticos con troyanos, virus y herramientas similares, acceso a datos confidenciales de muchos tipos). Algunas de estas acciones se denominan ciberataques, y pueden englobar a su vez varias formas de actuación. Una de ellas, muy conocida y puesta en práctica, es la comentada anteriormente de ataques de denegación de servicio o DoS.

Un ciberataque puede tener diversos objetivos; puede ir dirigido a ciudadanos individuales y anónimos, a ciudadanos concretos y conocidos, a alguna empresa privada de mayor o menor importancia, a entidades oficiales y/o gubernamentales, a infraestructuras críticas de un país o región, etc. Si el ciberataque llega a afectar a infraestructuras críticas o, si sin llegar a ello, tiene una envergadura suficiente como para poner en peligro el funcionamiento normal de una parte grande de la sociedad, el país afectado debe poner en marcha una serie de mecanismos de defensa para bloquear el ataque y recuperar sus funciones básicas. Eventualmente podría llegarse a la situación de producirse una respuesta en forma de contraataque por parte del país afectado, y

llegados a este punto se considera que se ha establecido una ciberguerra. Este escenario es hipotético, y aún no se ha llegado a producir claramente. Entre otros motivos para ello están algunos de los citados en el punto 2.3: en muchas ocasiones es muy difícil llegar al origen real de los ataques, debido a técnicas de ocultación usadas por los atacantes o a falta de colaboración por parte de algunos gobiernos, instituciones o proveedores de servicio para identificar el origen de cierto tráfico de red. En otras ocasiones, aun sabiendo desde dónde están llegando los ataques, no se puede culpar a los propietarios de los equipos que los llevan a cabo, pues pueden haber sido víctimas sin saberlo de algún tipo de infección maliciosa que haya tomado el control de dichos equipos. Por otra parte existe una reticencia constante por parte de los distintos gobiernos para admitir que están llevando a cabo operaciones de distinto tipo en el ciberespacio (como ejemplo, considérese los constantes ataques recibidos en E.E.U.U. que se consideran provenientes de China, aunque este país lo niega(22)). Todo esto hace que no sea fácil llegar a una situación de ciberguerra abierta, aunque sí es habitual que diariamente se estén produciendo acciones de ataque en el ciberespacio(23)(24)(25)(26), de igual manera que se realizan operaciones de espionaje en el mundo real y no se llegan a admitir públicamente.

Lo que sí se llega a admitir en general, a pesar de las delgadas líneas de separación que existen en determinadas situaciones y que impiden calificarlas dentro de uno u otro concepto, es que los ciberdelitos más habituales suelen ser perpetrados por elementos delictivos de los llamados tradicionales, mientras que los ciberataques de mayor escala que pueden afectar a un país o región son protagonizados por agencias nacionales o gubernamentales de distinto tipo. Este último caso equivale, en el terreno virtual de las redes de comunicaciones, a un ataque entre naciones o entre alguna facción extranjera y un determinado país. De acuerdo con todo lo anterior, se ha establecido una diferencia en el tratamiento de los distintos tipos de acciones ilegales en el ciberespacio, de tal manera que la lucha contra la ciberdelincuencia es responsabilidad de las distintas fuerzas y cuerpos de seguridad del estado correspondiente, y la prevención y en su caso respuesta ante ciberataques (es decir, la ciberdefensa) son competencia de las fuerzas armadas o cuerpos militares del entorno en cuestión.

En referencia a la ciberguerra hay opiniones divergentes respecto a la posibilidad de que sea factible, o respecto a qué entorno debe ser el que la protagonice. Es significativo que en el punto 2.12 de la estrategia de ciberseguridad del Reino Unido de 2009(27) se indique lo siguiente:

> *Hay un continuo y amplio debate respecto a lo que implica la 'ciberguerra', pero hay consenso en que, con una dependencia creciente del ciberespacio, la defensa y explotación de los sistemas de información son asuntos cada vez más importantes para la seguridad nacional. Reconocemos la necesidad de desarrollar capacidades militares y civiles, tanto a nivel nacional como con aliados, para asegurar que podamos defendernos frente a ataques, y tomar medidas contra los adversarios cuando sea necesario.*

2.6 INFRAESTRUCTURAS CRÍTICAS

Ya se han mencionado en anteriores puntos de este capítulo las infraestructuras críticas, y se ha dado una primera definición en el punto 2.2. Se ampliará ahora la definición, considerando por qué se incorpora en este Proyecto, analizando los sectores que son críticos en el funcionamiento normal de los países, comentando las características particulares de las infraestructuras críticas, mencionando los tipos de amenazas que pueden sufrir, algunos ejemplos de ataques y cómo se enfoca la protección de las infraestructuras críticas en España.

Para empezar, puede ser interesante ver cómo se definen las llamadas infraestructuras críticas (en adelante IICC) por parte de distintos organismos con objeto de tener una visión general de cómo se ven desde distintos puntos.

Según una directiva del Consejo de la Unión Europea destinada a la identificación de IICC (28):

> *Se entenderá por:*
>
> *a) «infraestructura crítica», el elemento, sistema o parte de éste situado en los estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;*
>
> *b) «infraestructura crítica europea» o «ICE», la infraestructura crítica situada en los estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras.*

Por otra parte, en E.E.U.U. se definen oficialmente las IICC en la llamada "USA PATRIOT Act"[14] de 2001 de la siguiente manera(29):

> *Las infraestructuras críticas son los activos, los sistemas y las redes, ya sean físicos o virtuales, tan vital para los Estados Unidos que su incapacitación o destrucción tendría un efecto*

[14] Aunque la expresión "USA *patriot*" significa patriota de EEUU, el nombre de la ley "USA PATRIOT" viene de ***U****niting and* ***S****trengthening* ***A****merica by* ***P****roviding* ***A****ppropriate* ***T****ools* ***R****equired to* ***I****ntercept and* ***O****bstruct* ***T****errorism*, es decir, "unir y fortalecer América proporcionando herramientas adecuadas necesarias para interceptar e impedir el terrorismo". Se promulgó el 26 de octubre de 2001, poco después de los atentados del 11 de septiembre en E.E.U.U.

> *debilitador sobre la seguridad, la seguridad económica nacional, la salud pública o la seguridad nacional, o cualquier combinación de los mismos.*

En el campo de las IICC no existe tanta disparidad en las definiciones como en otros términos mencionados en este proyecto. Hay un cierto consenso en lo que a la definición se refiere, así como en cuanto a qué sectores se pueden considerar críticos. También está claro que las consecuencias de cualquier incidencia en las IICC pueden ser graves: pérdidas materiales, pérdidas económicas, miedo de la población, aumento de la desconfianza de los ciudadanos en sus gobernantes, o incluso pérdida de vidas humanas llegado el caso (piénsese en un posible ataque al abastecimiento de agua o de material para hospitales durante un tiempo prolongado, o ataques a alguna infraestructura relacionada con la energía nuclear).

Las IICC abarcan multitud de sectores: energía, transporte, alimentación, abastecimiento de materias básicas, etc. Las distintas legislaciones aprobadas al respecto suelen indicar de manera genérica los sectores que se consideran especialmente importantes. De hecho, aunque suele haber listas generales que indican qué sectores de las infraestructuras existentes en cada país pueden ser críticos, el inventario de los recursos reales y concretos no suele ser público (en España, el llamado “catálogo nacional de infraestructuras estratégicas”, gestionado y mantenido por la Secretaría de Estado de Seguridad del Ministerio del Interior, tiene la clasificación de seguridad de “secreto”). Más adelante se mencionarán los sectores concretos que pueden considerarse críticos.

Las infraestructuras críticas tienen una serie de características que las hacen muy peculiares en su tratamiento. Para empezar, normalmente pertenecen a empresas privadas aunque, siendo propiedad privada, los distintos estados y organizaciones supranacionales se encuentran en la obligación de velar por su integridad y seguridad interviniendo en los planes de protección. El motivo está claro y se ha explicado, pero es interesante contemplar esta circunstancia que no se da en otras muchas empresas privadas que no entran en la categoría de críticas para el funcionamiento de un país y que, por tanto, no gozan de la misma atención. Queda claro que en este ámbito es fundamental la colaboración público-privada, en interés y beneficio mutuo, y en ese sentido las distintas reglamentaciones establecen la necesidad de una constante comunicación a las estructuras estatales de las características de las IICC, incidentes de seguridad registrados, planes establecidos, etc.

La caída de alguna IICC no sólo afecta a la población civil; también puede afectar a otros sectores críticos. Es esta dependencia intersectorial otra característica de las IICC que las hace aún más importantes si cabe. Piénsese por ejemplo en alguna situación problemática en el sector del transporte; esta situación puede afectar al de la salud y al del abastecimiento de bienes básicos de la población. Otros ejemplos son aún más claros: si es el sector de la energía el que sufre algún problema importante, afectaría totalmente al resto de sectores. Además, se pueden producir efectos en cadena, que alcancen y afecten zonas remotas respecto de las inicialmente perjudicadas, y estos efectos pueden incluso cruzar las fronteras. Tal es el caso del corte que en noviembre de

2006 dejó sin suministro eléctrico a varios millones de ciudadanos de Francia, Alemania, Italia, Bélgica y España(30), o de otro(31)(32) que afectó a unos 55 millones de ciudadanos en E.E.U.U. y Canadá el 14 de agosto de 2003[15]. Por estos motivos es importante disponer de planes de contingencia que procuren limitar la interdependencia entre sectores y que aseguren un mínimo de resiliencia (capacidad de asumir situaciones límite, resistir y recuperarse de ellas). Habitualmente se dispone de planes específicos para determinados sectores, como el energético o el de las comunicaciones.

Por otra parte, los problemas en algunas IICC pueden tener efectos a medio o largo plazo. La recuperación no tiene por qué ser inmediata, existiendo un tiempo de recuperación que puede ser mayor o menor en función del sector afectado y de la severidad de los problemas.

De todo lo comentado hasta ahora queda claro que la seguridad de las IICC es vital hoy en día, y precisamente por eso se consideran un posible objetivo de acciones de ciberterrorismo. En este ámbito hay que contemplar muy especialmente, y a diferencia de otros sistemas de información de tipo general, las dos vertientes principales de la seguridad, es decir, la seguridad física y la seguridad lógica. Ésta última viene obligada por el hecho de que los llamados "sistemas de control industrial" (en inglés ICS, *Industrial Control Systems*) para el control y gestión de las IICC se apoyan en sistemas informáticos y en redes de comunicación. Los ICS incluyen diversos tipos de sistemas, como los denominados SCADA[16], DCS[17] y PLC[18]. Antiguamente los sistemas de monitorización y control remotos se basaban en enlaces a través de redes telefónicas conmutadas, y se utilizaban protocolos propietarios (ICCP[19], DNP[20]). Actualmente se tiende a utilizar redes telemáticas con soluciones y protocolos de propósito general (incluso integrando en algunos casos las redes de control con las redes corporativas) que suponen mayor facilidad de despliegue, menor dependencia de fabricantes, compatibilidad entre equipos y un ahorro importante de los costes. El paso de los sistemas tradicionales y antiguos de control a los actuales ha traído ventajas añadidas a las indicadas (como mayor facilidad para controlar sistemas remotos desatendidos, menor necesidad de desplazamientos físicos, rapidez en el diagnóstico y localización de averías y en el mantenimiento y la gestión en general) pero también muchos inconvenientes. Entre éstos están la necesidad de las empresas de adaptar todo el

[15] Este corte se produjo por un fallo en el software de control de alarmas, que impidió que se redirigiera la distribución de energía de unas líneas sobrecargadas. Al no producirse la redirección, se produjo un efecto en cascada. Algún grupo islamista se atribuyó posteriormente la acción, aunque no está clara la autoría.

[16] *Supervisory Control and Data Acquisition, sistemas que permiten la* adquisición de datos, la supervisión de diversas variables y el control sobre determinados parámetros.

[17] *Distributed Control Systems*, sistemas de control distribuido

[18] *Programmable Logic Controllers*, controladores lógicos programables

[19] *Inter-control Center Communication Protocol*, protocolo para comunicación de centros de control

[20] *Distributed Network Protocol*, protocolo distribuido de redes

sistema de control y supervisión, con la consiguiente complejidad e inversión económica. Pero a efectos de la seguridad, el mayor de los inconvenientes es la aparición de nuevas vulnerabilidades que antes no existían.

Tradicionalmente, cuando se quería atacar a alguna IICC, era necesario realizar un desplazamiento físico al lugar en cuestión. En el caso de guerras, los objetivos militares solían contemplar, por ejemplo, el bombardeo de fábricas, líneas de suministro o centros de generación de energía del enemigo. Hoy en día se pueden realizar ataques similares sin la necesidad ni el riesgo del desplazamiento físico. Muchas de las vulnerabilidades propias de los sistemas informáticos de uso general se han trasladado al del entorno de las IICC, y si bien existen algunas diferencias entre los sistemas y redes de uso general y los dedicados a las IICC, en muchos casos se pueden explotar los errores y obtener ventajas similares. Como ejemplo, la empresa ReVuln ha publicado un video en el que muestra cómo explota varias vulnerabilidades de sistemas SCADA de conocidos fabricantes (General Electric, Schneider Electric, Kaskad, ABB/Rockwell, Eaton, Siemens) y consigue la ejecución remota de código, secuestros de sesión, descargas arbitrarias de ficheros y otras situaciones en absoluto deseables por los usuarios de los sistemas (33)(34).

Precisamente la aparición de nuevas vulnerabilidades en las IICC y la posibilidad de explotarlas es lo que hace atractivo para los terroristas este campo de actuación, y el motivo de que se estudien en este proyecto. El ciberterrorismo dirigido a las IICC constituye una nueva amenaza que debe ser afrontada por todos los países afectados, y que de hecho es objeto de mención en la mayoría de estrategias y políticas de seguridad, como se verá en el capítulo 4.

Se llega a la conclusión, por tanto, de que la seguridad de las IICC debe afrontarse en distintos frentes. La seguridad física ya se ha tenido presente desde hace décadas, y se puede suponer que los distintos gestores y propietarios de las IICC tienen experiencia y la han aplicado adecuadamente. Sin embargo no puede decirse lo mismo de la seguridad lógica, y no solo por la falta de experiencia histórica, sino por la constante evolución del mundo del cibercrimen en general y de las vulnerabilidades que continuamente salen a la luz (o no, y eso es lo peor) y que pueden ser explotadas. Esto exige aplicar al entorno de las IICC algunas de las metodologías existentes de análisis y gestión de riesgos: se deben identificar los activos importantes, analizar las vulnerabilidades y amenazas y el impacto eventualmente producido, para finalmente evaluar los riesgos con objeto de establecer salvaguardas adecuadas. Deben aplicarse medidas preventivas para minimizar los riesgos, pero también otras destinadas a reducir el impacto, haciendo cumplir los correspondientes planes de contingencia que las propias legislaciones obligan a elaborar.

Hay muchas similitudes entre las redes informáticas y de comunicaciones de uso general y los sistemas de control industrial o ICS, pero también hay factores diferenciadores, como los que se mencionan a continuación:

- Rendimiento: los sistemas ICS tienen unos requisitos más estrictos en cuanto al retardo de transmisión de la información, pero son menos exigentes en lo que al ancho de banda necesario se refiere;
- Disponibilidad: en los sistemas de control de las IICC se requiere una disponibilidad permanente. Acciones tan simples como un simple reinicio de un servidor, que pueden ser más o menos habituales en los entornos de uso general, pueden llegar a ser peligrosas en entornos críticos;
- Gestión de riesgos: en los entornos de uso general se pretende asegurar la integridad, confidencialidad y disponibilidad de los datos, así como la autenticación y el no repudio en ciertos casos. Los sistemas ICS requieren además contemplar la seguridad personal y la tolerancia a fallos;
- Arquitectura: en los sistemas ICS suele existir una arquitectura descentralizada en la que tienen vital importancia los elementos remotos (sensores, actuadores, etc.). Además, ciertos problemas en los elementos remotos pueden provocar fallos en cascada que aumenten el efecto de los problemas iniciales, algo que no es habitual en los entornos de uso general;
- Interacciones físicas: en el mundo TIC de uso general los cortes de servicio no suelen tener consecuencias físicas, sin embargo en el ámbito de los sistemas ICS sí pueden tenerlas (con mayor o menor repercusión en el usuario final del servicio);
- Criticidad en los tiempos de respuesta: en el ámbito del uso general de las TIC el control de acceso no suele influir en el funcionamiento de los sistemas. Por el contrario, considérese un caso en el que un operador de un sistema ICS deba introducir un usuario y una contraseña para controlar un equipo que está provocando un fallo grave y que pueda producir averías en otros equipos o incluso pérdidas de vidas humanas;
- Limitaciones de recursos: muchos sistemas ICS se basan en equipamientos que tienen capacidades muy limitadas en cuanto a recursos hardware o software. Esto hace que ante determinados problemas de seguridad no se puedan aplicar medidas que serían fáciles de aplicar en entornos de uso general;
- Productos "propietarios"[21]: los sistemas ICS suelen emplear protocolos de comunicación propietarios que impiden traspasar al mundo de las IICC algunas soluciones habituales en el ámbito de uso general. Lo mismo ocurre con algunos productos hardware, lo que impide la interconexión de elementos de distintos fabricantes;
- Gestión de cambios en el software: en el mundo del uso general de las TIC las respuestas a la mayoría de las vulnerabilidades suele producirse relativamente pronto, en forma de parches o actualizaciones. En los entornos ICS estos parches no se proporcionan de manera rápida, y además no siempre es posible su aplicación inmediata, debido a la importancia de los procesos involucrados y

[21] En entornos software, "propietario" es lo opuesto a "libre", y suele implicar restricciones para usarlo, modificarlo o redistribuirlo. Habitualmente su uso requiere una licencia con coste.

a la necesidad de probar previamente los posibles efectos secundarios que puedan producirse posteriormente;
- Ciclo de vida de los componentes: en el ámbito de uso general la esperanza de vida de los distintos componentes es relativamente pequeña. Esto implica que algunas vulnerabilidades pueden desaparecer con la inevitable sustitución de los elementos implicados que de cualquier manera se iba a realizar tarde o temprano. Los componentes de los sistemas ICS tienen una esperanza de vida mucho mayor, y su sustitución no es tan habitual ni tan sencilla como en el primer caso;
- Acceso físico a los componentes: algunos elementos de los sistemas ICS se encuentran físicamente muy alejados y distribuidos, lo que hace muy difícil su tratamiento o sustitución.

Las amenazas a las que están sujetas las IICC no solo proceden de ataques; también hay circunstancias que pueden provocar problemas en las propias herramientas de control y gestión, como errores en la programación o en la operación de los sistemas de control. Esto supone precisamente un posible punto de entrada para ciberterroristas que quieran acometer algún tipo de atentado. Además los ataques pueden venir desde el exterior de la infraestructura en cuestión, pero también pueden ser producidos por personal interno, o pueden colaborar a que alguien externo los lleve a cabo.

En cuanto a los sectores que engloban generalmente las IICC, suelen estar bien identificados. Hay mucha documentación al respecto; se mencionarán aquí un par de ejemplos de listas de sectores críticos.

En algunos casos la legislación va evolucionando y se va adaptando a la circunstancias, redefiniendo cuáles son los sectores críticos. En E.E.U.U. se promulgó el llamado Plan de Protección de Infraestructuras Nacionales(35) (NIPP, *National Infrastructure Protection Plan*) del Ministerio de Seguridad Interior (*Department of Homeland Security*) quese basaba en una directiva de diciembre de 2003 denominada HSPD-7 (*Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, Directiva Presidencial de Seguridad interior 7: Identificación, Priorización e Identificación de Infraestructura Crítica)(36) que identificaba 18 sectores como recursos e infraestructuras críticas. Posteriormente, en febrero de 2013 se aprobó la Directiva de Política Presidencial 21 sobre “seguridad de infraestructura crítica y resiliencia” (PPD-21) (37)(38) que dejó en 16 los sectores de infraestructura crítica:

- Sector químico (incluye productos para agricultura, sector farmacéutico, productos para el consumidor final y otros)
- Instalaciones comerciales
- Comunicaciones
- Fabricación de materiales críticos (industrias de fabricación de metales, fabricación de maquinaria, equipos eléctricos, fabricación de productos para aviación, fabricación de material ferroviario, etc.)
- Pantanos

- Base industrial de defensa (se refiere al complejo industrial que permite la investigación, desarrollo, diseño, producción, distribución y mantenimiento de sistemas y componentes de armamento militar; hay más de 100.000 empresas que trabajan con contratos para el Ministerio de Defensa de E.E.U.U.)
- Servicios de emergencia
- Energía (se contemplan 3 segmentos: electricidad, petróleo y gas natural)
- Servicios financieros
- Agricultura y alimentación
- Instalaciones del gobierno (incluye edificios, tanto en territorio nacional de E.E.U.U. como en el extranjero, para actividades comerciales, actividades de recreo, para almacenamiento de información, equipos, material, para usos militares especiales, embajadas, laboratorios, palacios de justicia, elementos de protección física como sistemas de control de acceso o circuitos cerrados de televisión, guarderías e instituciones de educación superior, museos nacionales y otros)
- Salud pública
- Tecnologías de la información
- Reactores nucleares, materiales y residuos
- Sistemas de transporte
- Agua (tanto abastecimiento como gestión de aguas residuales)

En España para hablar de la protección de IICC es necesario remontarse al 7 de mayo de 2007, cuando la Secretaría de Estado de Seguridad del Ministerio del Interior aprueba el primer Plan Nacional de Protección de Infraestructuras Críticas. Se definió también el primer "Catálogo Nacional de Infraestructuras Estratégicas" bajo el control del posteriormente creado Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC). Con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas. Tras la aprobación de la directiva europea 2008/114/CE del Consejo Europeo(28), se transpone al ordenamiento jurídico español dicha directiva por medio de la Ley 8/2011 de 28 de abril(39)por la que se establecen medidas para la protección de infraestructuras críticas (conocida como LPIC). Esta ley desarrolla entre otras cosas la creación de determinados centros de coordinación, y define los sectores estratégicos siguientes:

- Administración
- Espacio
- Industria nuclear
- Industria química
- Instalaciones de investigación
- Agua
- Energía
- Salud
- Tecnologías de la información y las comunicaciones
- Transporte

- Alimentación
- Sistema financiero y tributario

Poco después, concretamente el 20 de mayo, se aprueba el Decreto 704/2011 que realiza el desarrollo reglamentario de la Ley 8/2011. Así pues, nuestro país dispone ya de una infraestructura legal que soporta distintos organismos dedicados a la protección de las IICC.

Llegados a este punto, cabe preguntarse: ¿realmente es posible que se produzca interrupción de servicios esenciales debido a algún fallo en infraestructuras críticas? ¿Ha ocurrido algún caso real? ¿Es viable un ataque ciberterrorista que produzca daños físicos?

Se han producido numerosos casos de ataques contra equipamiento relacionado con IICC, aunque no siempre han afectado a los sistemas de control o ICS. En un artículo del 27 de agosto de 2009(40), el "*Journal of Energy Security*" (Periódico de Seguridad de la Energía) indica que "*el sector de la energía de E.E.U.U. experimentó una media de 1280 ciberataques significativos en cada uno de los primeros seis meses de 2002*". No especifica si los ataques iban dirigidos a modificar o anular los sistemas de control de las propias infraestructuras o si por el contrario sus objetivos eran equipos o información de las distintas redes corporativas de las compañías eléctricas (para obtener información de clientes, de facturación, etc.). Otro caso similar(41)(42) fue la infección con el virus "*Shamoon*" (también conocido como "*Disstrack*") de tres cuartas partes (en total unos 30.000) de los equipos corporativos de la compañía Saudi Aramco el 15 de agosto de 2012, provocando destrucción masiva de ficheros en los discos duros. En este caso la red corporativa estaba separada de la red de control de infraestructuras. El mismo virus se utilizó menos de dos semanas más tarde contra la empresa RasGas Company en Catar(43)(44). Un artículo del periódico *The Wall Street Journal* de abril de 2009 afirmaba que la red eléctrica de E.E.U.U. había sido invadida por espías (45). De acuerdo con esa información, ciberespías de China, Rusia y otros países podrían haber introducido en los sistemas ICS algún tipo de software que en el futuro podría usarse para provocar daños si fuera necesario. Las fuentes de la noticia eran funcionarios de la administración de seguridad nacional en activo y otros que lo fueron anteriormente. Según se dice, muchas de las intrusiones no fueron detectadas por las compañías que operan las IICC, sino por agencias de inteligencia del país. En febrero de 2011 McAfee publicó un informe sobre la operación "*Night* Dragon": al parecer, desde noviembre de 2009 se estaban produciendo ataques continuados, originados en China, contra compañías relacionadas con el sector de la energía (gas, petróleo) de E.E.U.U., Grecia, Taiwan y Kazajistán. No fueron comprometidos los sistemas ICS, pero sí los corporativos, y se robaron muchísimos archivos de correos electrónicos y documentos sensibles. En noviembre de 2012 la empresa alemana especializada en energías renovables 50Hertz sufrió un ciberataque que duró 5 días; fue un ataque de denegación de servicio utilizando una red zombi o *botnet*[22]. Se bloquearon sus dominios y toda la conectividad

[22] Se definen y analizan las redes zombi o *botnets* en el punto 3.5.6.

de la empresa con Internet, dejando inoperativo su correo electrónico(46). Aunque en los casos comentados no se llegara por parte de los atacantes a los sistemas de control industrial, no deja de ser significativo que los equipos relacionados (directa o indirectamente) con las IICC sean blancos de ataques, dada la importancia que la información obtenida pueda tener quizá para posteriores ataques ciberterroristas. Un informe de McAfee (47) indica que en una encuesta realizada a responsables de redes relacionadas con IICC de 14 países en el año 2010 el 80% de los encuestados se había enfrentado a algún ataque de denegación de servicio a gran escala, y el 85% había sufrido infiltraciones en sus redes.

Ha habido mucha discusión sobre si un ciberataque puede tener consecuencias físicas, como daños en equipos. Para comprobar este extremo, en 2007 el Ministerio de Energía de E.E.U.U. realizó lo que se conoció como el "Test Aurora" con objeto de comprobar si se podía llegar a dañar físicamente algún equipo solo con un ataque por software. Se hicieron las pruebas en el Laboratorio Nacional de Idaho, propiedad del citado ministerio. En ellas se consiguió destruir un generador de energía que funcionaba con combustible diesel. Los generadores tienen unos parámetros de funcionamiento, entre ellos ciertas frecuencias, voltajes y fases en la rotación de sus ejes. Suelen tener relés de protección que actúan cuando alguno de estos parámetros se sale de unos márgenes, pero también hay tolerancias en cuanto a los valores nominales de funcionamiento. Esto permite que durante un determinado intervalo de tiempo se permita a un sistema volver a su funcionamiento anormal tras algún fallo puntual o durante la puesta en marcha. El ataque realizado consistía en llevar el generador fuera de sincronismo durante estos intervalos de tiempo, provocando finalmente el fallo físico. Se realizó un vídeo que se distribuyó a la agencia de noticias Associated Press en el que se veía un generador que empezaba a temblar y que finalmente llenó la habitación de humo antes de dejar de funcionar. En la Figura 2-2se muestran algunos fotogramas del citado vídeo.

Pero la capacidad de provocar daños físicos en equipos no ha quedado en el laboratorio: ya se ha producido en entornos de producción: un ejemplo es el conocidísimo caso de Stuxnet.

Stuxnet(48)(49)(50) es un gusano[23] que fue identificado en junio de 2010. Infectó a millones de ordenadores de todo el mundo, aunque era inofensivo salvo que el equipo infectado cumpliera ciertas condiciones. Aprovechaba vulnerabilidades de sistemas Windows de Microsoft. Estaba diseñado para propagarse a través de distintos medios (memorias USB, recursos compartidos de red, bases de datos SQL) pero solo actuaba si el sistema infectado cumplía con unas determinadas características: debía tener instalado un software de control SCADA de Siemens (llamado "Step 7"). Este software sirve para reprogramar unos dispositivos PLC (*Programmable Logic Controllers*,

[23] Se denomina "gusano" a un tipo de software que se copia a otros equipos sin intervención humana y sin alterar los ficheros existentes.

controladores lógicos programables) que se encargan de controlar a otros dispositivos de la instalación nuclear, concretamente unos convertidores de frecuencia que a su vez determinan las revoluciones por minuto a las que trabajan unas centrifugadoras. Cuando los operadores del sistema querían programar los PLC, los conectaban a las máquinas Windows infectadas. Ahí el gusano hacía un ataque del tipo "hombre-en-el-medio"[24], enviando una programación a los PLC distinta de la que el operador había establecido, aunque luego le informaba de que la programación se había realizado correctamente. Como resultado se modificaban las revoluciones de trabajo de unas centrifugadoras para enriquecer uranio en instalaciones nucleares. Lo curioso e interesante es que no ponía a trabajar al equipo a unas revoluciones que directa y rápidamente provocaran una avería, sino que subía el régimen de trabajo a unos valores altos pero dentro de lo especificado por el fabricante. Todo esto en conjunto hacía que los fallos en los equipos fueran apareciendo gradualmente, no de golpe, y así se facilitaba pensar en la posibilidad de que los equipos hubieran venido defectuosos de fábrica. A la vez se conseguía eliminar la sospecha de la existencia de algún ataque de tipo informático, lo cual permitía a Stuxnet seguir infectando más equipos. En total fueron unas 1000 centrifugadoras las que se vieron afectadas por el gusano antes de que se descubriera su existencia.

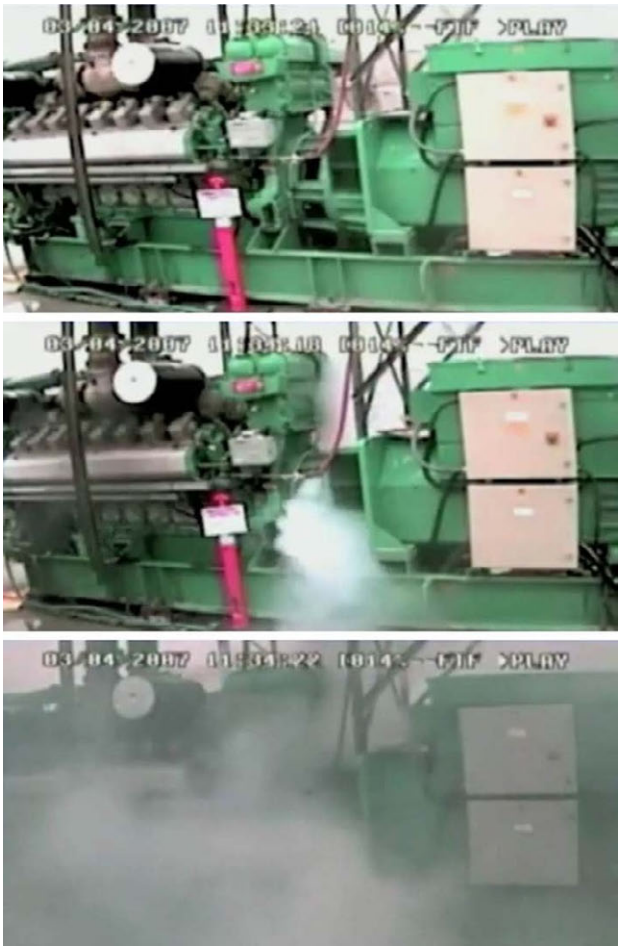


Figura 2-2: Fotogramas del vídeo del "Test Aurora"

Stuxnet constituye un ejemplo de ataque dirigido a un objetivo concreto, por eso se le denomina en muchos textos "arma software". De hecho estaba diseñado para atacar, por el procedimiento indicado en el párrafo anterior, solo a los modelos de PLC S7-315 y S7-417 de Siemens. Y no solo eso: los ataques solo se producían si los PLC estaban

[24] Conocido como "*Man in the* Middle", o MitM, consiste en interponerse en la comunicación entre dos elementos, haciendo que toda la comunicación pase por el elemento intermedio, que captura todos los datos intercambiados.

configurados para controlar a un número determinado de convertidores de frecuencia (recuérdese que son los que modifican las revoluciones por minuto de las centrifugadoras). Pero además se tenía que cumplir otro requisito: que los convertidores de frecuencia hubieran sido fabricados por la compañía iraní *Fararo Paya* o por la finlandesa *Vacon*. Con todos estos condicionantes, se da por hecho que el objetivo eran las instalaciones nucleares de enriquecimiento de uranio de la compañía Natanz en Irán. La sofisticación del diseño del gusano era extrema: aprovechaba vulnerabilidades que no se conocían previamente hasta que se descubrió el propio gusano y se analizó a fondo. Stuxnet incorporaba drivers para Windows que habían sido firmados con certificados válidos robados probablemente de Realtek Semiconductor Systems y JMicron Technology Corp. Su implementación incluía técnicas avanzadas para evitar su análisis y hacer que fuera difícil aplicar ingeniería inversa. No se conoce su autoría, aunque muchos apuntan a que se podría haber diseñado en Israel y posiblemente con colaboración de E.E.U.U.(51)(52)(53).

No ha habido (o no se conocen) nuevos casos de gusanos similares, pero el diseño de Stuxnet ha supuesto un avance extraordinario en cuanto a la sofisticación respecto a otro tipo de *malware* usado por otros ciberdelincuentes, y demuestra que hoy en día este tipo de ataques es posible. Muestra de ello es una situación que no se ha explotado (o al menos no se conoce que se haya hecho): en 2011 se descubrió que en China había sistemas SCADA que presentaban una vulnerabilidad que podía ser aprovechada con fines maliciosos. El software llamado *KingView*, desarrollado por la empresa Beijing Wellin Control Technology Development sirve para visualizar procesos en sistemas ICS, y se usa en la industria china en multitud de ámbitos, incluyendo industrias aeroespaciales y de defensa nacional (véase la Figura 2-3). La última (por entonces) versión de *KingView* tenía una vulnerabilidad de desbordamiento de montículo[25]. Este fallo fue descubierto por el investigador Dillon Beresford, quien lo comunicó a la empresa fabricante y al CN-CERT[26], sin respuesta de ninguno de ellos por cierto(54)(55).

El caso de Stuxnet no es el único conocido en el que alguna acción exterior a la infraestructura crítica produce efectos nocivos. En el año 2000 se produjo en Australia un incidente protagonizado por Vitek Boden, que trabajaba para la empresa Hunter Watertech, dedicada a instalar sistemas SCADA para control de aguas residuales en el Consejo Maroochy Shire. Al cesar en su empresa tras una relación tensa, solicitó trabajo en el propio Consejo de Maroochy Shire, sin éxito. Como venganza decidió realizar acciones utilizando los sistemas que probablemente él mismo habría montado. Montó en su coche un sistema de radio robado y un ordenador. En al menos 46 ocasiones, entre el 28 de febrero y el 23 de abril de 2000, se acercó a distintas áreas y envió órdenes remotas aprovechando el sistema de control por radio. Provocó el vertido de más de 800.000 litros de aguas residuales en varios parques, ríos y en los jardines de un

[25] El desbordamiento de montículo se llama en inglés *heap overflow*, y es distinto del desbordamiento de pila o *stack overflow*. Ambos son tipos de *buffer overflow* o desbordamiento de *buffer*.

[26] CN-CERT es el equipo de respuesta a emergencias informáticas de China.

hotel. Gran cantidad de animales marinos murieron, el agua de un arroyo se volvió prácticamente negra y el mal olor se hizo insoportable(56)(57). En este caso, la seguridad de acceso de los sistemas SCADA vía radio no estaba configurada de manera adecuada, y no era necesario tener conocimientos profundos de programación para diseñar e implementar una solución como el gusano Stuxnet, sino simplemente explotar la vulnerabilidad del acceso radio.

Figura 2-3: Software KingView

CAPÍTULO 3 USO DELICTIVO DEL CIBERESPACIO

Una vez se han establecido algunas definiciones y conceptos importantes que se usarán en este trabajo, y teniendo en cuenta la importancia del ciberespacio para la sociedad moderna y las particulares circunstancias que rodean las acciones cibercriminales, es conveniente entrar en detalle sobre las acciones delictivas que se llevan a cabo. En particular, se hablará en este capítulo sobre los distintos tipos de cibercriminales que existen, definiendo términos habitualmente empleados en el mundo de la seguridad para designarlos; a continuación se hablará sucintamente sobre la clasificación legal de los distintos delitos cometidos en el ciberespacio, pero únicamente a efectos de dar una primera idea sobre los mismos, pues los aspectos legales se analizarán con más detalle

en el punto 4.3. Después se hará un repaso de las herramientas utilizadas en el mundo del cibercrimen y el ciberterrorismo, para a continuación explicar las técnicas y procedimientos asociados a las distintas herramientas. Se ha considerado que esta forma de dividir todo el conjunto de recursos de los cibercriminales puede ayudar en la comprensión de sus operaciones y formas de trabajar, aunque en muchos textos se mezclan herramientas y técnicas.

Es interesante también mencionar algunos de los numerosos grupos que operan ilegalmente en el ciberespacio en distintos ámbitos, comentando algunas de sus acciones y sus formas de actuación. El siguiente punto está dedicado a la llamada "web profunda" o "web oculta", una parte del ciberespacio donde los cibercriminales se comunican entre sí, obtienen y venden herramientas y servicios varios, y preparan sus acciones; la llamada "criptomoneda" es otro aspecto analizado en el mismo punto, por ser una nueva faceta que está tomando una enorme importancia en la economía mundial y que sirve de gran ayuda para el mundo del cibercrimen. Por último, se analizarán las consecuencias económicas del cibercrimen, lo que dará una justificación de la importancia de combatirlo adecuadamente.

3.1 TIPOLOGÍA DEL CIBERDELINCUENTE

Una de las cuestiones que ocupan a los investigadores del cibercrimen es el perfil del ciberdelincuente y del ciberterrorista. Realmente no puede hablarse de un único modelo: son varios los que existen, y cada uno de ellos tiene un perfil psicológico, una motivación y una serie de características distintivas. No hay un margen de edades concreto de los cibercriminales, entre otras cosas porque pueden utilizar las herramientas como medio de comisión de delitos y también como objetivo. En este último caso, no es habitual encontrar cibercriminales de una edad avanzada, dado lo relativamente novedoso de este tipo particular de delitos. Tampoco existe un nivel de estudios determinado, pero sí hay diferencias entre los distintos perfiles existentes en cuanto a conocimientos técnicos de las TIC y en cuanto a las razones para cometer distintos ciberdelitos. Se hablará a continuación de una primera clasificación en función de las habilidades técnicas en el mundo TIC; acto seguido se comentarán los distintos tipos de ciberdelincuentes según las motivaciones de cada uno. Se usarán en muchos casos términos en inglés por ser los más habituales y no existir para ellos traducción al español.

Se habla a menudo en los medios especializados de los ***hackers***. En general se les define como personas con unos conocimientos técnicos muy avanzados que son capaces de vulnerar la seguridad de sistemas lógicos o físicos; pueden encontrar agujeros de seguridad, o vulnerabilidades, y aprovecharlas para realizar alguna acción, no necesariamente maliciosa. En este sentido, muchos de los descubrimientos de los *hackers* han sido beneficiosos para la comunidad de usuarios y desarrolladores de sistemas. Gracias al conocimiento de los fallos de seguridad, se han podido idear y aplicar parches y soluciones que han protegido al usuario final de estos fallos, y a los desarrolladores de los efectos secundarios que pudiera haber (como pérdida de

credibilidad y, consecuentemente, pérdidas económicas). Hace algunas décadas, cuando aún no estaban tan desarrollados y extendidos los sistemas informáticos, los *hackers* solían buscar fallos en sistemas sencillos, como los telefónicos; era la época del *phreaking* (término que puede proceder de *phone* y de *freak*[27]). Los ***phreakers*** solían buscar un beneficio económico, realizando por ejemplo llamadas telefónicas sin coste en una época en la que dichas comunicaciones no eran gratuitas. Los *hackers*, como herederos de los *phreakers* pero actuando en sistemas más evolucionados que la nueva informática acercaba al usuario, no tenían inicialmente ese componente motivacional de provecho económico, y se movían por impulsos de curiosidad e incluso ayuda a la comunidad. Sus intenciones no eran nocivas y atendían más a la satisfacción de superar retos o al deseo de reconocimiento público que a obtener beneficios fuera de la propia popularidad. Muchos incluso realizaban sus investigaciones por hobby. La imagen pública de los *hackers* no era mala, y a ello contribuía en buena medida la aparición de obras literarias y cinematográficas que ensalzaban sus acciones beneficiosas. Además, se produjo en ciertos casos un "efecto llamada" por la posibilidad de ser contratado por alguna empresa importante tras haber demostrado unos conocimientos extraordinarios. Esta circunstancia no era exclusiva de hace un par de décadas: recientemente Apple contrató a uno de los desarrolladores más brillantes que consiguió romper la seguridad de su sistema operativo móvil iOS[28]. Según el periódico *The Guardian*, uno de cada cuatro *hackers* trabaja ahora para algún organismo federal de E.E.U.U., aunque no está claro si esto ocurre por motivos de retribuciones adecuadas o por amenazas de cárcel si no aceptan la oferta(58)(59).

Un concepto similar al de *hacker* es el de ***cracker***[29]. En este caso, este perfil de usuario intenta "romper" un sistema y aprovecharlo en muchos casos para usos para los cuales no estaba diseñado (por ejemplo saltando la protección de algún software para que no requiera licencia legal, o permitiendo que consolas de juegos puedan ejecutar aplicaciones no originales). Habitualmente la acción realizada es ilegal, y tiene como objetivo obtener algún beneficio o infligir daño; los *hackers* que no tenían intenciones ilícitas empezaron a utilizar el término *cracker* para distinguirse de ellos, ya que el *hacking* tradicional no tenía tales objetivos. Debe tenerse en cuenta que originalmente el *hacker* se consideraba un ciudadano legal, con unos ideales e incluso un código ético definidos, pero no se consideraban delincuentes (aunque sus acciones fueran ilegales). Con el tiempo, los términos tienden a confundirse, y actualmente se llama *hacker* de manera genérica a cualquier persona que consiga burlar la seguridad de algún sistema, sea cual sea su objetivo y sus motivaciones. Para distinguir el objetivo o las

[27] *Freaky* es un término en inglés que suele hacer referencia a personas que, en su aspecto o en su comportamiento, son peculiares y distintas al resto. El diccionario de la RAE lo recogerá en su 23ª edición como "friki", con el significado de "extravagante, raro o excéntrico".

[28] De nombre Nicholas Allegra pero conocido mundialmente por el apodo Comex, se hizo especialmente popular al conseguir romper el sistema operativo iOS simplemente visitando una página web desde un iPhone. Fue contratado por Apple en 2011, cuando tenía 19 años.

[29] Hay fuentes que indican que *cracker* viene del verbo inglés *crack* (romper); otras dicen que viene de *criminal hacker*.

motivaciones, actualmente es frecuente encontrar los términos *hacking ético* para referirse a aquellas actividades que no buscan beneficio ni causar daño; los *white hackers* o *white hats* (en español serían *hackers* de guante blanco) son los que practican el *hacking* con fines buenos, y los *black hackers* o *black hats* son los *crackers*.

Hay aficionados que utilizan alguna herramienta realizada por los *hackers*, directamente o modificándola ligeramente, aunque luego pueden y suelen presumir de haber entrado en los sistemas atacados. Son los llamados ***script kiddies*** o ***noobs***. En este caso no se trata de verdaderos expertos, ya que no encuentran vulnerabilidades, sino que simplemente ejecutan alguno de los *exploits* (programas que aprovechan alguna vulnerabilidad de algún sistema para entrar en él o provocar algún tipo de modificación o provecho al respecto) publicados o los modifican, haciendo sus propios *scripts* o pequeños programas interpretados. Un término similar empleado a menudo en los entornos de Internet es ***lammer***, que hace referencia a las personas que fingen ser expertos (y a los que les gusta que se les denomine *hackers*) pero realmente no tienen ni siquiera unos conocimientos mínimos en el ámbito de la seguridad informática. A pesar de su falta de conocimiento interno de los sistemas no hay que desdeñar su importancia, ya que a menudo son protagonistas de ciertos ataques o acciones ilegales, y además de convertirse en ciberdelincuentes, entorpecen la labor de investigación de las fuerzas de seguridad en la búsqueda de los autores originales de las herramientas ilegales.

Estos perfiles comentados, caracterizados por sus conocimientos técnicos, corresponden a los que investigan en la parte más interna de los distintos sistemas, tanto hardware como software, pero no necesariamente son los ciberdelincuentes que realizan acciones ilegales (aparte de la propia modificación de sistemas). El mundo del cibercrimen está formado además por otros actores que, en la mayor parte de las ocasiones, son los que provocan directamente los daños en las víctimas, y que se pueden clasificar según motivaciones de diversa índole que les lleva a realizar sus acciones. Así, se pueden encontrar los llamados ***hacktivistas***, término que designa a aquellas personas que realizan acciones que se valen de las TIC para realizar alguna reivindicación, protesta o defensa de algún tipo de idea; a tales actividades también se le denomina de manera general ciberactivismo. Las motivaciones de los ciberactivistas pueden ser políticas, religiosas, sociales, éticas o de otro tipo. La definición del término *hacktivismo* tampoco está demasiado clara, y de hecho en algunos entornos se incluye a los ciberterroristas dentro de ese concepto, dado que realizan sus acciones defendiendo ideas políticas o religiosas igualmente. Los ciberactivistas pueden realizar acciones de manera rutinaria o bien respondiendo a acontecimientos concretos. Esta actividad no es nueva; un ejemplo de ello ocurrió ya en 2001: tras un incidente aéreo en la zona del Mar de China entre un avión militar de reconocimiento de E.E.U.U. EP-3 y dos cazas J-8 de China, el piloto de uno de los cazas tuvo que lanzarse y desapareció, dándose oficialmente por muerto. Se produjo una situación de mucha tensión entre ambos países, dado que el avión estadounidense tuvo que realizar un aterrizaje de emergencia y la tripulación estuvo varios días en poder del gobierno chino. En el ciberespacio hubo respuesta por parte de ambos bandos, ya que *hacktivistas* chinos y norteamericanos se dedicaron a atacar

diferentes servidores web del otro país, publicando mensajes de denuncia al otro bando y defendiendo sus respectivas posiciones(60).

Otro entorno que provoca a menudo problemas en el ciberespacio son los propios **empleados o ex-empleados** de empresas e instituciones. Es conocido que uno de los factores de riesgo que puede provocar fugas o destrucción de información son los empleados que, descontentos por diversos motivos (situación laboral, sueldo bajo, despido, condiciones de trabajo o no estar de acuerdo con decisiones de la empresa, entre otros) deciden vengarse de alguna manera, ya sea filtrando información a otras empresas, gobiernos o servicios de información, ya destruyendo información o equipos. Otra motivación aparte de la venganza por algún motivo concreto suele ser el móvil económico, ya que en muchos casos los empleados acceden a alguna proposición externa a cambio de una suma muy elevada de dinero.

Los propios gobiernos de los países, o bien organizaciones internas (servicios de información, unidades militares) también pueden cometer acciones ilícitas en el ciberespacio. La más habitual es la infiltración en sistemas de otros países (incluso aliados) para obtener información. Es la versión TIC del espionaje tradicional, y lógicamente recibe el nombre de **ciberespionaje**. En muchos casos se pretende obtener información en general; en otros, se busca algún tipo de dato concreto, con objetivos políticos, militares o incluso industriales. En este sentido ha sido muy conocido el caso de espionaje por parte de China a E.E.U.U.; de acuerdo con un informe confidencial redactado para el gobierno norteamericano y filtrado al periódico *The Wall Street Journal*(61)(62), China ha conseguido obtener gran cantidad de documentación de diseño y operación de distintos sistemas de armas (misiles Patriot, caza F/A-18, avión convertible V-22 Osprey, helicóptero Black Hawk, y el avanzadísimo caza F-35).

Además de todos los grupos anteriores, existen también los ciberdelincuentes que pertenecen al llamado **crimen organizado**; suelen estructurarse en bandas que hacen uso de las nuevas tecnologías para obtener principalmente beneficios económicos, usándolas como medio de sus actividades ilícitas o como fin en sí mismo, aunque también se cometen otro tipo de delitos. A modo de ejemplo se pueden citar delincuentes especializados que realizan timos por Internet, otros que consiguen credenciales bancarias de usuarios para extraer luego el dinero de sus cuentas, los que usan los medios de comunicación para acosar sexualmente a menores o distribuir material relacionado con esta práctica, aquellos que utilizan las herramientas desarrolladas por *hackers*/*crackers* para secuestrar ordenadores y pedir un rescate por poder volver a usarlos, etc. Hay que tener en cuenta que en el mundo del cibercrimen existe cierta especialización, de tal manera que hay personas o grupos que se dedican a encontrar vulnerabilidades en los sistemas y a programar código que las explote, otros que compran estas herramientas para utilizarlas directamente o bien para montar infraestructuras destinadas a proporcionar servicios delictivos, otros que alquilan o contratan estos servicios, etc.

Por último, existen otros tipos de ciberdelincuentes, algunos de ellos ocasionales, que incluso puede que no sepan que están cometiendo un delito: a veces se realizan

acciones en forma de experimentación o puesta en práctica de ciertos conocimientos (que pueden haber sido aprendidos en unos minutos buscando rápidamente en Internet) que implican infracción puntual de las leyes nacionales del sujeto que las realiza. Piénsese, por ejemplo, en algo tan sencillo[30] como averiguar la clave de una red inalámbrica que no esté configurada adecuadamente. Esta acción puede tipificarse como un delito de acceso ilícito a un sistema o a una red, a pesar de que algunos usuarios de redes no lo sepan, pues la llevan a cabo con objeto de poder navegar desde su domicilio o lugar de trabajo donde no tengan acceso inalámbrico autorizado. En otros casos, los usuarios que disponen de una red inalámbrica y han detectado que alguien está utilizándola sin permiso deciden capturar el tráfico de los intrusos para poder averiguar su identidad o tomar represalias; esta medida también es ilegal, pues se considera interceptación ilícita. También hay quien accede a algún servidor público de Internet para comprobar las vulnerabilidades en el software del servidor, incluso con la intención de avisar a los administradores de que sus sistemas tienen agujeros de seguridad. Estas acciones, aunque tengan objetivos loables, también son constitutivas de delito: salvando las distancias, es comparable a (e igual de ilegal que) entrar en el domicilio de otra persona para avisarle de que no tiene medidas de seguridad que lo impidan.

A modo de resumen y de manera general, la clasificación que se encontrará en multitud de documentos oficiales e informes diversos relacionados con el cibercrimen y la seguridad de redes en general es la indicada según las motivaciones de los intervinientes, es decir, se suelen realizar habitualmente menciones a:

- organizaciones estatales
- grupos del crimen organizado
- grupos *hacktivistas*
- delincuentes ocasionales y aislados

[30] La facilidad que ofrece Internet para conseguir información hace que sea extremadamente fácil buscar alguna guía sencilla para, por ejemplo, encontrar claves de redes Wifi. Además, las herramientas para hacerlo están disponibles de manera gratuita. Por tanto, cualquier persona sin excesivos conocimientos técnicos puede averiguar la clave de ciertas redes Wifi que no estén correctamente protegidas.

3.2 CLASIFICACIÓN LEGAL DE CIBERDELITOS

Con objeto de poder evitar, perseguir y, en su caso, sancionar adecuadamente las diversas formas de delito llevadas a cabo alrededor de los sistemas y redes de comunicaciones e informáticos, es necesario realizar una definición y clasificación recogidas en algún texto legal. En función del marco legal que se considere, los tipos penales concretos podrán variar. En el capítulo 4 se analiza con más detalle la legislación existente en distintos ámbitos nacionales e internacionales al respecto, pero se considera conveniente introducir en éste cuáles son, de manera general, los posibles ciberdelitos que se pueden cometer y castigar. De esta forma, cuando en el punto 3.3 se describan las actuaciones habituales de los cibercriminales, se podrán englobar y asociar a algunos de los tipos penales descritos en este punto.

Una de las clasificaciones de los ciberdelitos que ha quedado como referencia en todo el mundo es la que se describe en el llamado "Convenio sobre la Ciberdelincuencia"(63)(64) aprobado por el Consejo de Europa en 2001[31] (más conocido como Convenio de Budapest). En él se dan unas directrices para adoptar, en cada país que quisiera ratificarlo, una legislación adecuada para tratar el cibercrimen, y así poder disponer de una serie de disposiciones legales más o menos uniformes entre países. Aunque se hablará de él en el punto 4.3, se indican a continuación los tipos de ciberdelitos que establece el convenio:

1. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
   1.1. Acceso ilícito: se refiere al acceso a todo un sistema o a parte de él, infringiendo medidas de seguridad, con intención de obtener datos informáticos o con otra intención delictiva; considera también el caso de sistemas informáticos interconectados. Un ejemplo puede ser instalar algún programa de control remoto a algún usuario sin su consentimiento, con objeto de acceder a su información privada.
   1.2. Interceptación ilícita: hace referencia a la obtención de datos en tránsito en transmisiones no públicas, incluyendo emisiones electromagnéticas, con intención delictiva. Un caso posible podría ser el uso de algún analizador de paquetes de red o *sniffer* para conseguir datos sensibles o privados.
   1.3. Ataques a la integridad de los datos: provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.
   1.4. Ataques a la integridad del sistema: se refiere este caso a la provocación de fallos en el funcionamiento de sistemas e incluso la inutilización de los mismos. Un ejemplo podría ser el ataque de denegación de servicio (DoS) a un servidor web con objeto de dejarlo inoperativo, como se comentó en la página 18.

[31] Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión n° 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

1.5. Abuso de los dispositivos: este tipo de delito parece muy ambiguo, pero se entenderá mejor mencionando los casos contemplados y algún ejemplo:
   1.5.1. Producción, obtención, difusión o posesión de dispositivos o programas diseñados para cometer alguno de los delitos contemplados en los apartados 1.1 a 1.4 anteriores (ejemplo: programación de un *keylogger*[32] para obtener credenciales de acceso a datos bancarios de un usuario, o sea, para conseguir un acceso ilícito), y también:
   1.5.2. Difusión de contraseñas que permitan acceder a un sistema informático con objeto de cometer algún delito de los indicados en los apartados 1.1 a 1.4 anteriores (ejemplo: facilitar a alguien la contraseña de acceso de un usuario a su ordenador personal, con objeto de obtener datos particulares, lo cual sería un ejemplo de acceso ilícito).

2. Delitos informáticos.
   2.1. Falsificación informática: hace referencia a la manipulación (introducción, alteración, borrado) de datos informáticos que a su vez provoque que en un sistema se generen datos falsos, con intención de que sean tomados como ciertos en procesos legales. Ejemplo: falsificación de algún tipo de certificado modificando la fecha de emisión.
   2.2. Fraude informático: este tipo de delito tiene como condiciones que se cause perjuicio patrimonial a alguna persona y que haya intención además de obtener beneficio económico por parte de otra. Los casos más habituales son los timos en Internet, algunos de los cuales se describirán más adelante.

3. Delitos relacionados con el contenido.
   3.1. Delitos relacionados con la pornografía infantil: se incluye la producción, oferta, puesta a disposición, difusión, transmisión, adquisición y posesión usando sistemas informáticos.

4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

5. Otras formas de responsabilidad y de sanción.
   5.1. Tentativa y complicidad: se deben tipificar como delitos los actos de complicidad deliberada con otros para cometer alguno de los delitos antes expuestos, así como los intentos de cometer alguno de estos delitos.

Éstos son algunos de los ciberdelitos que se pueden cometer usando las TIC; como se ha dicho antes, es una lista que ofrece una guía para que cualquier país pueda legislar

[32] Un *keylogger* es un programa maligno que captura las pulsaciones que se realizan en un teclado sin que el usuario del equipo sea consciente. Se suele usar para obtener contraseñas y credenciales de acceso a sistemas.

respecto al cibercrimen, con una clasificación completa y unas definiciones claras del alcance de cada infracción. La lectura del convenio no indica en palabras llanas cuáles son los delitos descritos (lo cual es lógico, dado el carácter del documento), y por ese motivo se han añadido algunos ejemplos para aclarar a qué se refiere cada tipo. En el siguiente punto se indicarán más ejemplos generales de hechos delictivos que se han llevado o se están llevando a cabo en el ciberespacio, y se mencionarán o explicarán casos concretos y conocidos. Se podrá ver que cada acción ilícita tiene su reflejo en alguno de los apartados anteriores del Convenio de Budapest, lo cual puede despejar las dudas respecto a si determinada acción es susceptible de ser castigada o, dicho de otra manera, si podría ser legal o ilegal. Téngase en cuenta, no obstante, que el Convenio representa una referencia, que ha debido ser trasladada a la legislación nacional correspondiente para que los actos delictivos puedan ser perseguidos y castigados. Además, el texto legal aprobado por cada país debe contemplar la intención delictiva en cada uno de los casos (como menciona el propio Convenio en sus descripciones de ciberdelitos), pues si no fuera así, la simple posesión de un *sniffer* o programa de captura de paquetes para solucionar algún problema técnico podría llegar a ser considerada delito.

3.3 ACTOS DELICTIVOS HABITUALES EN EL CIBERESPACIO

Hay una gran cantidad de ciberdelitos que no requieren el uso por parte de los delincuentes de herramientas especiales ni grandes conocimientos técnicos o de programación. El desconocimiento por parte de una gran base de usuarios en el ciberespacio de la existencia de engaños, unido a la excesiva confianza mostrada por muchas de las víctimas, en parte debido a ese desconocimiento, hace que los cibercriminales puedan llevar a cabo sus acciones y sacar provecho. La imaginación de los delincuentes es el único límite que puede encontrarse en este terreno. Se inventan continuamente formas de embaucar a los usuarios en Internet, y cuando las fuerzas de seguridad descubren las técnicas en uso e impiden hasta cierto punto que se sigan utilizando, se inventan otras nuevas. La mayoría de los usuarios medios de Internet no están al tanto del modus operandi de los ciberdelincuentes, y eso es lo que permite a éstos seguir con sus engaños.

Uno de los campos en los que más triunfa la ciberdelincuencia es el de los **timos y fraudes en el comercio electrónico**. Es indudable que la existencia de una red mundial de datos que permite la comunicación instantánea de millones de personas en todo el mundo ha posibilitado el auge del comercio electrónico, la posibilidad de consultar características técnicas de productos, la comparación de precios y la compra sin salir de casa. Desgraciadamente también se ha facilitado que exista un terreno aprovechado a diario por estafadores para conseguir dinero o bienes.

El fraude en comercio electrónico presenta muchas variantes. Una de ellas es la existencia de ciertos portales web de venta con apariencia normal. Un usuario descuidado puede realizar compras de artículos que nunca se le van a enviar, a pesar de haber realizado el pago correspondiente. Puede parecer difícil establecer una

infraestructura para llevar a cabo este engaño y salir indemne, ya que podría suponerse que el estafado puede denunciar el hecho y los delincuentes serían perseguidos y castigados. En España es obligatorio indicar determinados datos en las páginas web que permitan realizar actividades económicas o lucrativas (denominación social, NIF, domicilio, dirección de correo electrónico, etc.)[33]. Sin embargo, no todas las webs de venta por Internet tienen estos requisitos, ya que cada país impone unos distintos. Esto permite que este tipo de fraudes sean posibles y habituales. El hecho de que los ciberdelincuentes se encuentren en otro país, que se les haya hecho alguna transferencia de dinero a cuentas en el extranjero, y que en ocasiones sea difícil perseguir a los responsables o hacer algún seguimiento del destinatario del dinero (debido, a veces, a la poca colaboración de ciertos proveedores de servicio y de algunos gobiernos) son factores que facilitan enormemente la comisión de este tipo de delitos.

De manera similar se producen acciones parecidas en los portales de compraventa entre particulares, subastas y anuncios clasificados: los vendedores timan a los compradores, no enviándoles la mercancía. Aquí se ofrecen a menudo productos a muy bajo precio y en condiciones muy ventajosas en cuanto a gastos de envío, devoluciones, período de pruebas, etc. Se le exige un adelanto al comprador, diciéndole que cuando el pedido llegue a su poder deberá pagar el resto. El pedido nunca llega, y el comprador pierde el dinero adelantado. En otros casos es aún peor, ya que no se les pide un adelanto a los compradores, sino el importe íntegro de la transacción. Para proteger a los futuros compradores algunos portales suelen tener sistemas de puntuación, de tal suerte que cuando un vendedor realiza una transacción, el comprador puede valorar diversos aspectos (rapidez en la transacción, respuesta del vendedor ante dudas del comprador, fidelidad del producto recibido respecto a lo anunciado, etc.). De esta manera "se le pone una nota" (se puntúa) al vendedor, y en caso de que no sea fiable, es poco probable que en el futuro encuentre compradores. Esto lo solucionan los delincuentes generando nuevas cuentas con distintas identidades cada vez. Una táctica usada por los ciberdelincuentes en muchos casos es hacer copias de anuncios reales que aparecen en otros portales de venta reconocidos y de prestigio. Los estafadores llegan a copiar los textos y las fotos de los artículos del portal original, incluso en muchos casos se ponen en contacto con el vendedor real del artículo para a su vez poder facilitar datos reales y fiables a las víctimas. Con el paso del tiempo los productos implicados en estas transacciones fraudulentas se han ido adaptando: se suelen vender productos de alta tecnología, vehículos, artículos exclusivos… Estos artículos se venden a precios notablemente más bajos de lo esperado. Se suelen buscar motivos creíbles para vender a precio tan bajo los productos de alta gama; así por ejemplo, en el caso de vehículos, se recurre a la excusa de que el vehículo es de empresa y ha sido adquirido a bajo precio por el vendedor pero éste ha sido destinado de pronto a otro país, teniendo que deshacerse del vehículo con prisas; también se indica a veces que el vendedor pertenece al cuerpo diplomático y lo ha podido conseguir a bajo precio pero debe cambiar de

[33] Según la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, conocida como LSSI (Ley 34/2002 de 11 de julio)

embajada. Todo esto genera en la víctima del fraude una falsa sensación de seguridad y le lleva a caer en la trampa.

Una circunstancia adicional que se produce a veces es la venta de productos ilegales, como medicinas, drogas, títulos o licencias falsos, etc. Tras iniciarse la transacción y realizarse el pago por parte del comprador, no se le envía lo solicitado, y éste no lo denuncia dado el carácter ilegal del producto que pretendía adquirir, con lo que el estafador sale indemne de la operación.

Otro campo en el que se cometen fraudes es el de los medios de pago, en estrecha relación con los casos anteriores comentados. En ocasiones, para generar confianza a los compradores, se les ofrece que una entidad haga de intermediaria, para facilitar el pago y asegurar que el dinero no le llega al vendedor si antes éste no ha puesto a disposición el artículo de venta. La supuesta empresa intermediaria, conocida habitualmente como *escrow* (o empresa de servicio de depósito de garantía), ofrece al comprador que éste le entregue el dinero de la compra, y le dice que exigirá al vendedor que entregue el artículo a dicha empresa intermediaria. Una vez ésta dispone en su poder de ambos conceptos (dinero del comprador y artículo del vendedor), la empresa intermediaria hará llegar a cada uno lo que espera. Sin embargo, el artículo que espera el comprador estafado nunca se le entrega, ya que las empresas *escrow* son ficticias o, aun sin serlo, suelen pertenecer al propio vendedor, y de hecho son parte de su infraestructura de engaño. También se utilizan empresas *escrow* falsas en el sentido contrario, es decir, para engañar a un vendedor, que envía su producto a dicha empresa pero que finalmente no recibe el dinero de la venta. Estos timos existen desde hace bastantes años (véase artículo de 2002 de NBC News en (65)). Es importante saber que la existencia de intermediarios o *escrow* no es ilegal, y de hecho su existencia y funcionamiento están regulados. En Europa, la Comisión Europea publicó en el año 2007 la Directiva de Sistemas de Pago, PSD 2007/64/EC(66) (PSD, *Payment Services Directive*)[34]. Esta normativa proporciona una base legal para establecer la llamada "zona única de pagos en euros", o SEPA (*Single Euro Payments Area*). Además permite, entre otras cosas, la creación de servicios de depósito de garantía de bajo costo en Internet, debidamente controlados y regulados por los respectivos gobiernos. El propio portal *ebay* permite trabajar con estas empresas intermediarias de depósito de garantía, aunque recomienda mucha cautela a la hora de elegir alguna(67).

Otra variante que merece la pena mencionar es el fraude con cheques de caja. Este tipo de documento se considera seguro y con garantía, ya que es una orden de pago que un banco realiza tras comprobar que existen fondos. Se utiliza de manera fraudulenta para engañar a vendedores particulares en Internet. Lo habitual es que un falso comprador se interese por el producto, pero le indique al vendedor que no se lo va a pagar directamente, sino que lo hará alguien que reside en el país del vendedor y que le debe

[34] La directiva europea ha sido incorporada al ordenamiento jurídico español por medio de la Ley 16/2009 de 13 de noviembre, el Real Decreto 712/2010 de 28 de mayo y la Orden EHA/1608/2010 de 14 de junio.

dinero al comprador. A éste se le hace llegar un cheque de caja falso, y por un valor bastante superior al del importe del artículo vendido. Se le dice que el exceso de dinero es para cubrir gastos de envío, y que el dinero sobrante se le devuelva al comprador mediante transferencia. El comprador ingresa el cheque en su cuenta e inicialmente le aparece el abono, tras lo cual realizará la transferencia al estafador. Realmente el cheque estará retenido hasta que se pueda verificar el talón, operación que suele tardar varios días. Cuando la entidad financiera descubre que el cheque no tiene fondos, retira la cantidad de la cuenta del vendedor, pero ya es tarde porque posiblemente éste le haya hecho la transferencia al estafador. Un esquema parecido de engaño es el que utiliza ofertas de empleo muy atractivas, en las que una empresa internacional ofrece trabajar en casa por una elevada cantidad de dinero. A la víctima interesada en la oferta se le pide diversa documentación oficial e incluso se le hace un contrato falso. Se le indica además que la nómina se la pagará una empresa de su propio país que a su vez le debe dinero a la falsa empresa internacional; el motivo esgrimido es que ésta no tiene infraestructura en el país de la víctima y no desea disponer allí de cuentas bancarias para evitar complicaciones fiscales. De acuerdo con esta situación, se le envía a la víctima un cheque falso por un valor muy superior al de su nómina, y éste debe ingresarlo en su cuenta y a continuación devolver el dinero sobrante a la empresa internacional mediante una transferencia. Con un poco de suerte para los timadores, esta transferencia se hará antes de que se descubra que el cheque que se le facilitó a la víctima era falso. La transferencia realizada habrá utilizado dinero de la cuenta del ciudadano estafado.

También se realizan fraudes con intermediarios de compras: algunas empresas internacionales ofrecen a particulares en Internet convertirse en socios para actuar como intermediarios, con la excusa de que no desean establecer una infraestructura en el país del socio por motivos de ahorro de costes. De esta manera el intermediario (la primera víctima, ya que no será la única) debe anunciar en portales conocidos de Internet productos de gama alta a precios muy competitivos. Algún comprador interesado en un artículo realizará la compra; le pagará directamente al intermediario y éste enviará el dinero de la compra a la empresa internacional mediante una transferencia a algún banco (habitualmente de Europa Oriental). La empresa de los ciberdelincuentes enviará supuestamente la mercancía al comprador directamente, evitando de esa manera al intermediario problemas de almacenaje de productos. Esta es solo la teoría, pues la realidad es que nunca se le envía nada al comprador, de manera que éste, la segunda víctima del engaño, denunciará al intermediario, que también ha sido estafado.

A propósito de los delitos que conllevan engaño, ya se comentó en la página 17 el llamado **timo de las cartas nigerianas**: se envían a potenciales víctimas diversas comunicaciones (por correo electrónico, fax o correo ordinario) indicándole que una persona ha fallecido en algún país lejano sin herederos, y se dispone de una inmensa fortuna, de la cual la víctima puede llevarse un porcentaje; para ello debe aportar algún dinero con objeto de pagar tasas, facilitar trámites e incluso para algún que otro soborno, con la promesa de que recuperará ese dinero con creces. Este fraude también se conoce como el fraude del 419, en referencia al artículo del código penal de Nigeria

que lo contempla. Normalmente la procedencia de estos timos está localizada en países de África.

En estrecha relación con el anterior se encuentra el **timo de las loterías**: se hace creer a las víctimas del engaño que han ganado algún premio de una lotería, pero para cobrarlo deben aportar dinero con objeto de realizar ciertos trámites. Estos timos también proceden de África habitualmente, pero no solo de allí: también se han recibido correos electrónicos de ese tipo alegando proceder de la Sociedad Estatal Loterías y Apuestas del Estado de España; este organismo ha tenido que publicar en su sitio web un aviso sobre estafas por suplantación de identidad, como se puede ver en la Figura 3-1, aclarando algunos conceptos y dando consejos para defenderse de esa estafa(68).

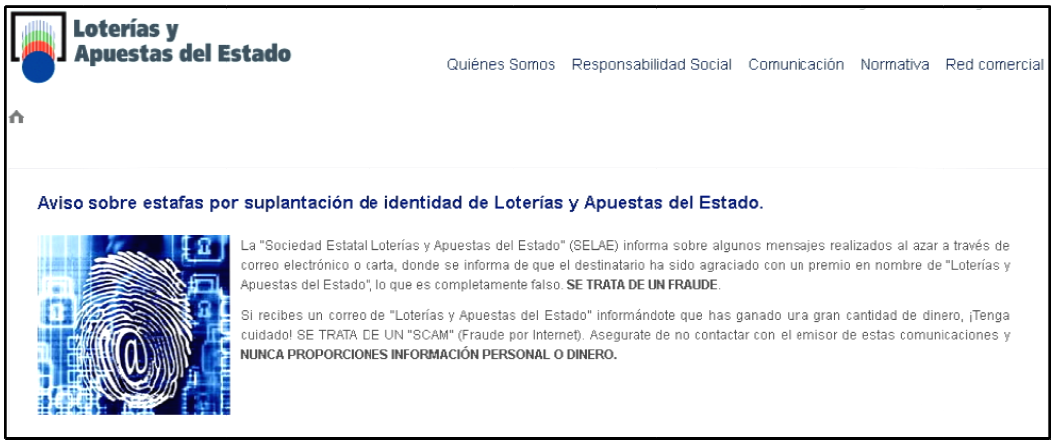


Figura 3-1: Aviso de Loterías y Apuestas del Estado sobre estafas

Hay una amplia variedad de engaños similares a los que se acaban de exponer, con situaciones creíbles y que demuestran que la imaginación de los ciberdelincuentes es inagotable. En todos los esquemas de trabajo anteriores hay un punto que no habrá pasado desapercibido: ¿cómo reciben los estafadores el dinero de sus víctimas? Si lo hacen mediante alguna transferencia bancaria bastará con denunciar el hecho ante las autoridades policiales y seguir la pista del titular de la cuenta de destino. Sin embargo esto no es tan fácil: los ciberdelincuentes se valen en el mundo del fraude en el ciberespacio, al igual que en otros ámbitos criminales, de personas denominadas mulas. El diccionario de la Real Academia de la Lengua Española define mula como “contrabandista de drogas en pequeñas cantidades”. En el ámbito del cibercrimen se denomina mulas a las personas utilizadas como intermediarios que reciben el dinero transferido por las víctimas de las estafas, y se encargan de traspasar este dinero mediante distintos métodos (en metálico, usando entidades de envío internacional de fondos o mediante posteriores transferencias) a los delincuentes, que pagan a las mulas una comisión por el trabajo realizado. Las organizaciones criminales suelen establecer una red de mulas en distintos países; inicialmente se desplazaban componentes de dichas organizaciones al país en cuestión, con diversas identidades falsas. Ahí abrían varias cuentas bancarias que servían para realizar el traspaso del dinero. Posteriormente, estas personas se dedicaron a captar a otras que les hicieran el trabajo (convirtiéndose los captadores en los llamados “muleros”); habitualmente se elegía a

inmigrantes del mismo país, que se encontraban en situaciones precarias y que aceptaban el trabajo por el poco esfuerzo exigido y los beneficios obtenidos a cambio. Otra casuística encontrada a menudo es la de las mulas que realizan el trabajo por obligación, al proceder de inmigración ilegal e incluso haber viajado al país engañadas, tras lo cual se les retira toda la documentación y se les obliga a intermediar entre estafados y delincuentes. También existen las mulas que no son conscientes de estar colaborando en operaciones de engaño, pues se les ofrece trabajo desde casa realizando tareas administrativas y ofimáticas con buenas condiciones de retribución(69)(70). Este último caso es peculiar en cuanto a la posibilidad de ser condenado por colaboración, ya que en el código penal español se indica que no hay delito sin dolo o imprudencia, y diversos tribunales fallan de distinta forma al respecto(71). En España el Grupo de Delitos Telemáticos de la Guardia Civil alerta periódicamente de este hecho(72), como se puede ver en la Figura 3-2. En el caso de los inmigrantes es difícil continuar con la pista para llegar a los estafadores, ya que aquéllos son habitualmente formados para afrontar las eventuales situaciones de detención por la policía. Habitualmente se aducen motivos de recepción de herencias o similares desde sus países de origen. Además, dado que se suele elegir a mulas sin muchos recursos económicos, las bandas criminales aprovechan esa circunstancia para obligarlas a realizar el trabajo, amenazándolas de distintas maneras si rehúsan hacerlo o lo denuncian a las autoridades.

Se observa pues que para cometer los ciberdelitos comentados hasta ahora es necesaria una mínima infraestructura técnica y humana. La técnica exige en algunos casos disponer de equipamiento de servidores donde alojar los falsos portales de venta o las empresas *escrow* ficticias. Esto conlleva además la contratación de subdominios en Internet, habitualmente en países con poco control policial y escasa colaboración con el resto de países en caso de realizarse investigaciones en éstos. En otros casos no es necesaria tal infraestructura: para intentar el engaño de las cartas nigerianas basta con realizar envíos masivos de correos, aunque luego se deben crear documentos falsos para enviárselos a las víctimas y que éstas crean que realmente existe una herencia, por ejemplo. A esto se le une la necesaria infraestructura de mulas o intermediarios, que debe renovarse constantemente, ya que a una determinada mula no se le puede aprovechar más que para dos o tres transacciones, con objeto de que no llame la atención el hecho de que haya excesivos movimientos en sus cuentas.

Figura 3-2: Aviso del Grupo de Delitos Telemáticos de la Guardia Civil sobre falsas ofertas de empleo para el blanqueo de dinero

En relación con los asuntos de engaño, existe otro delito consistente en provocarle al usuario de sistemas informáticos algún tipo de miedo o angustia, mediante el *malware* conocido como ***scareware***[35]. Un ejemplo muy típico es hacer creer a usuarios no expertos que un virus ha infectado su equipo, y que deben comprar un tipo concreto de antivirus falso; realmente ni existe el virus, ni el antivirus que el usuario compra realiza tal función(73). A veces se encuentran variantes en cuanto a la forma de hacer llegar el aviso falso al usuario: algunos vecinos de una ciudad de E.E.U.U. se encontraron, en 2009, con falsos avisos de multa en los parabrisas de sus coches, supuestamente por estar mal estacionados. Estos avisos daban indicaciones a los dueños para que visitaran una página web donde podrían ver fotos de la infracción. Al visitar la página, se invitaba a las víctimas a descargar e instalar una barra de herramientas con la cual podrían buscar su vehículo entre las fotos disponibles. La herramienta era realmente un tipo de *scareware* que mostraba una alerta de seguridad por un virus ficticio e invitaba a descargarse un falso antivirus(74).

Otro delito habitual que en ocasiones está ligado a los fraudes en compras y en comercio electrónico es el denominado *carding*, consistente en el uso ilegítimo, con ánimo de lucro, de tarjetas de crédito o débito ajenas. Esta actividad engloba tanto el uso de tarjetas de crédito falsas como utilizar las tarjetas físicas obtenidas por cualquier medio, además del uso de numeración de tarjetas sin disponer de ellas físicamente. Debe tenerse en cuenta que en muchos portales de venta por Internet basta con dar la numeración y la fecha de caducidad, así como el CVV o CVV2[36], para poder realizar operaciones comerciales. ¿Cómo se puede conseguir numeración de tarjetas de crédito o débito sin tenerlas? Existen foros relacionados con el cibercrimen que permiten comprar paquetes de información relativa a tarjetas de crédito, que incluyen los códigos CVV y CVV2 (ver Figura 3-3 como ejemplo de uno de estos foros). La obtención de datos

[35] *Scareware* procede del inglés *scare*, miedo, y de software.

[36] CVV significa *Card Verification Value*, es decir, valor de verificación de tarjeta. Es una serie de dígitos impresos en el reverso de las tarjetas de crédito y débito, que sirve para verificar, en compras por Internet o por teléfono, que quien haga uso de la tarjeta de crédito la tiene en su poder.

de tarjetas de crédito reales se puede hacer por *skimming*, nombre que hace referencia a un conjunto de técnicas usadas por delincuentes para conseguir dichos datos, por ejemplo copiando la banda magnética de las tarjetas al ser usadas en comercios o cajeros automáticos de entidades bancarias (se explicará con más detalle en el punto 3.5.2, página 77). También se pueden conseguir datos de tarjetas de crédito extrayéndolos de sitios web con poca seguridad; tal es el caso del robo de datos de 46 millones de tarjetas de crédito de unas cadenas de tiendas de ropa y artículos de decoración, ocurrido en E.E.U.U. en 2007(75). Sony también fue víctima de un robo similar en abril de 2011; se sustrajeron datos de cuentas de usuarios de la red PlayStation Network, así como una base de datos secundaria de números de cuentas bancarias, tarjetas de crédito y débito que, según Sony, estaba obsoleta(76). En fechas más recientes (principios de octubre de 2013) la empresa Adobe fue víctima del robo de datos de unos 38 millones de usuarios. Entre la información obtenida por los ladrones están los números de tarjeta de crédito; aunque esos números se encontraban cifrados, estando en poder de los cibercriminales son susceptibles de ser obtenidos en claro si se utiliza algún ataque eficiente(77). Con la información de las tarjetas se suelen realizar compras en Internet, o bien se hacen transferencias de dinero o disposición del mismo en cajeros automáticos. Una posibilidad al hacer transferencias de dinero es emplear mulas, como se comentó anteriormente en referencia a otro tipo de ciberdelitos.

Otro delito habitual es el **robo de información**; consiste en la obtención por medio del engaño, con la colaboración expresa de la víctima aunque sin que ésta sea consciente de ello, de credenciales de acceso a distintos servicios o de información confidencial en general. El nombre de la técnica empleada para ello es ***phishing***[37]. El caso más habitual es el de robo de información para operaciones en sitios web bancarios: los ciberdelincuentes configuran un servidor web idéntico al portal de entrada de alguna entidad bancaria conocida; suelen copiar hasta el mínimo detalle las páginas web, algo que no es nada difícil. A las víctimas potenciales se les envían correos electrónicos en los que se asegura que el remitente es el banco real, y se les solicita que entren en el portal de la entidad para confirmar de manera rutinaria los datos de usuario, o incluso se les dice que es necesario para evitar alguna acción de ciberdelincuentes que pueden supuestamente haber robado credenciales. La víctima accede al servidor web falsificado e introduce sus credenciales, que quedan ya en poder de los cibercriminales. A partir de ahí la operación más habitual es realizar transferencias de dinero a distintas cuentas. Por tanto la técnica del *phishing* sirve para obtener de manera genérica información de los usuarios y credenciales de acceso, y según qué tipo de credenciales se hayan obtenido, se podrán cometer diversos delitos. Uno de ellos es el **fraude en la banca electrónica**, ya comentado, pero puede haber otros. Esta técnica es una de las principales amenazas hoy en día; un informe de Symantec de 2013(78) indica que, de acuerdo con los datos obtenidos por sus productos de seguridad, uno de cada 414 correos electrónicos que se

[37] El término *phishing* tiene similitud con *fishing*, pesca; efectivamente, se intenta "pescar" información de las víctimas.

intercambian es de *phishing*. Más adelante en este trabajo se analizará con más detalle esta técnica (véase la página 73).

El caso comentado implica robo de información de acceso con colaboración de la víctima por ignorancia y utilizando el engaño. Hay otros casos de robo de información en los que no se engaña a la víctima para que introduzca sus credenciales en una página web falsa, sino que se utiliza diverso tipo de *malware* que se instala en los equipos de las víctimas. El robo de información se puede producir a ciudadanos particulares de manera aleatoria, o bien puede ir dirigido a extraer datos específicos de empresas, gobiernos o instituciones. De manera genérica se considera esta situación como un delito de **ciberespionaje**; lo habitual es utilizar como herramienta algún virus o troyano o gusano, o bien infraestructuras APT (*Advanced Persistent Threat*, amenaza persistente avanzada), que serán explicadas en el punto 3.5.7.

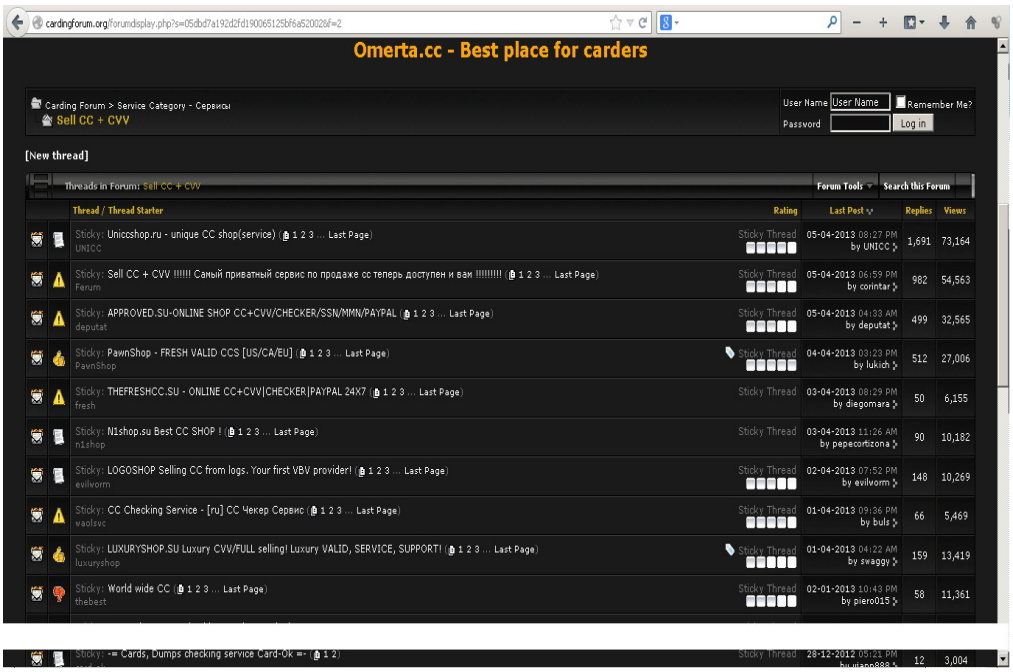


Figura 3-3: Foro donde se pueden comprar y vender datos de tarjetas de crédito

Una evolución, o mejor una consecuencia, del robo de información puede ser el delito de **robo de identidad**. Este tipo de delito está en aumento en todo el mundo. Según el Wall Street Journal, ya en 2009 se produjeron 9'9 millones de casos de robos de identidad en E.E.U.U.(79). El informe de Symantec de 2013 mencionado anteriormente(78) indica que la mitad el *malware* creado en 2012 tenía como objetivo robar información personal o hacer un seguimiento de las actividades de los usuarios. De esta manera se pretende obtener datos familiares, números de teléfono marcados o de los que se hayan recibido llamadas, datos de los contactos personales, información de conocidos en el ámbito de la empresa, información financiera, credenciales de acceso a diversos servicios en Internet o en redes corporativas, hábitos de la vida diaria, aficiones, etc. Con toda esta información se suelen realizar posteriormente acciones en

nombre de la víctima, es decir, el ciberdelincuente se hace pasar por ella, aportando incluso datos personales que le permiten hacer creer que realmente es la víctima quien está actuando. Se consigue así también anonimato para cometer otros delitos, como lavado de dinero negro o tráfico de drogas. En otros casos se utiliza la identidad de alguien conocido para publicitar un negocio falso: es el caso de una abogada de Tejas cuyo nombre de soltera, dirección de la oficina y partes de su biografía personal fueron utilizadas para publicitar un despacho de abogados ficticio(80). Una vez obtenidos suficientes datos de una víctima, las formas de explotarlos son muy variadas.

El robo de identidad también puede ser la primera parte de un delito de **extorsión**, ya que puede darse el caso de que el cibercriminal tenga acceso a cierta información o pueda llegar a alterar las claves de acceso a ciertos servicios (no necesariamente bancarios). En esta situación, le pedirá a la víctima el desembolso de una cantidad de dinero para permitirle volver a tener acceso a los servicios en cuestión. La extorsión no solo se realiza tras conseguir información privilegiada de ciertos usuarios, es decir, tras el "secuestro de información"; también puede y suele llevarse a cabo mediante el secuestro de equipos. Hay un tipo de *malware* denominado genéricamente *ransomware*[38] que impide el uso normal de los equipos informáticos una vez han sido infectados. Para poder volver a tener su control, el usuario víctima debe realizar pagos a los cibercriminales. Ha habido muchos ejemplos de este *malware*; un caso muy conocido que se ha descubierto en otoño de 2013 es el *ransomware* llamado CryptoLocker. En la Figura 3-4 puede verse una captura de pantalla de un equipo infectado con este software dañino, que será analizado con más profundidad posteriormente (página 72).

[38] *Ransomware* viene del inglés *ransom*, rescate, y de software.

Figura 3-4: Aviso del *ransomware* CryptoLocker

Hay otros ciberdelitos consistentes en la **utilización ilícita de equipos** con distintos objetivos. La posibilidad que brinda a los cibercriminales disponer de equipos para aprovecharlos directamente o bien para utilizarlos como plataforma de cara a ulteriores acciones delictivas es inmensa. Se comentarán solo algunas opciones utilizadas.

El mundo de la publicidad y de los anuncios es otro de los que se han visto afectados por el fraude. En los medios tradicionales de comunicación (prensa escrita, TV) un anunciante paga simplemente por tener un anuncio publicado, sin saber si ha hecho efecto o no en los consumidores de esos medios. Hoy en día, con las nuevas tecnologías, las nuevas formas de llegar al usuario y la interactividad con éste, es posible conocer si un anuncio o campaña publicitaria hacen efecto verdaderamente. En multitud de sitios web existen anuncios que llevan al navegante a sitios externos al de la propia página web. Cuando un usuario llega a una página web de un anunciante, existen maneras de saber si ha llegado ahí directamente o bien si se le ha redirigido desde alguna otra página. Esto ha llevado a un modelo de negocio en el que el anunciante paga al publicador o proveedor de la página web en función de cuántos usuarios han pulsado ("han hecho clic") en el anuncio, algo que se puede considerar justo, ya que se supone que el proveedor ha facilitado que la publicidad haya sido efectiva y se haya visitado el sitio anunciado. Con el tiempo el modelo ha evolucionado y se han creado empresas que hacen de intermediarias entre anunciantes y publicadores (por ejemplo Google AdWords(81)). En este entorno del mundo de la publicidad en Internet ha surgido el llamado **fraude del clic**. El fraude consiste en pulsar en estos anuncios masivamente, bien por parte del defraudador, bien por personas contratadas (normalmente a bajo precio) para hacerlo, o bien usando equipos comprometidos de otros usuarios para realizar los clic de manera automática, sin que realmente hayan respondido a visitas

reales de usuarios del portal web. De esta manera el anunciante debe pagar elevadas sumas de dinero al publicador o a la empresa intermediaria de publicidad. Esto genera unas pérdidas que en muchos casos son millonarias. En 2007 Google aseguraba que perdía anualmente 1.000 millones de dólares por este tipo de fraudes(82). Un ejemplo de *malware* que realizaba estas acciones de manera automatizada es el conocido como Clickbot.A(83). Para conocer su funcionamiento, así como más detalles del negocio de la publicidad en Internet, puede consultarse el documento "*The Anatomy of Clickbot.A*"(84).

También se aprovecha la utilización ilícita de equipos para realizar ***ataques a servidores*** en general (web, FTP[39], etc.). Se comentó en la página 18 en qué consistía la denegación de servicio, enviando muchas peticiones a un servidor hasta que no pueda atenderlas y se interrumpa el servicio proporcionado. Este ataque a un servidor puede hacerse desde un solo equipo que sea el que envía millones de peticiones, pero es más efectivo si son miles o millones los equipos que a su vez inundan al servidor atacado con peticiones simultáneas. En ese caso es más seguro que el ataque pueda tener los efectos deseados, y además se consigue un anonimato que no existiría si fuera un solo equipo el que realizara la acción. A este tipo de operación se le denomina denegación de servicio distribuido (DDoS, *Distributed Denial of Service*). Esos miles o millones de equipos para lanzar ataques de manera voluntaria pueden haber sido comprometidos con algún *malware* que hace que, sin que los usuarios sean conscientes, estén participando en esa acción ilegal. Más adelante, en este mismo capítulo (punto 3.5.6, página 88), se analizará este aspecto con más detalle.

Otra posibilidad de utilización ilícita de equipos es usarlos para **propagar *malware***. Hasta ahora se ha estado utilizando este término de forma genérica para hacer referencia a cualquier software que tiene intenciones delictivas. ¿Cómo llega este software dañino a los equipos de millones de usuarios en todo el mundo? Hay diversas formas, como se explicará en el punto 3.4, pero como adelanto sirva decir que una de las maneras es utilizar como plataformas de inyección los equipos ya infectados de otros usuarios.

También se usan equipos ajenos comprometidos para enviar correos electrónicos de forma masiva para determinados intereses; a esto se le denomina de forma general ***spam***[40]. Esta técnica se usa para hacer llegar a millones de usuarios correos electrónicos en los que se intenta infectarles con algún tipo de *malware* o bien se pretende convertirles en víctimas de fraudes como el de las cartas nigerianas o el de las loterías. Si se enviaran todos esos correos electrónicos desde un único equipo de Internet sería relativamente fácil identificar el origen de estas comunicaciones. Para los ciberdelincuentes es más efectivo e interesante utilizar equipos comprometidos de otros

[39] FTP significa *File Transfer Protocol*, protocolo de transferencia de ficheros.

[40] Se denomina *spam* al envío masivo de mensajes de correo electrónico a millones de usuarios, con objeto de llevarles a algún tipo de engaño, o bien enviando contenido malicioso en forma de algún *malware* como adjunto, o bien con enlaces a direcciones web donde se aloja *malware* o donde se compromete de alguna manera el equipo del usuario.

usuarios. Esto es bastante habitual; como ejemplo, durante los primeros meses del año 2013 millones de usuarios del correo electrónico del proveedor Yahoo fueron víctima de una vulnerabilidad del tipo XSS (*Cross-Side Scripting*)(85) existente en muchos navegadores web que hizo que sus cuentas fueran secuestradas temporalmente y utilizadas para enviar *spam*(86)(87).

Como se puede deducir, la posesión temporal de equipos ajenos de manera ilícita suele valer como soporte y apoyo para la comisión de otros delitos de los comentados antes. Realmente no siempre hay una línea de actuación directa y lineal, sino que los ciberdelincuentes utilizan varias técnicas encadenadas para llegar a sus últimos objetivos.

Otra categoría de ciberdelitos es el que tiene que ver con la integridad de la información. Bajo este epígrafe se incluyen diversas actividades, como por ejemplo el llamado ***defacing*** o ***defacement***. En español suele denominarse desfiguración y consiste en modificar las páginas de un servidor web sin la autorización de los propietarios, para mostrar alguna información que les interese a los atacantes, o para redirigir a los visitantes a algún otro servidor. Suele ser el soporte de distintos tipos de protesta (*hacktivismo*, comentado anteriormente en la página 46, por ideologías políticas, religiosas, etc.), aunque también puede realizarse por motivos económicos. Un ejemplo de *defacing* es el que se llevó a cabo contra la web de *Hewlett Packard* a finales de 2012; un *hacker* autodenominado *Hitcher*, miembro del grupo de *hackers* paquistaníes PCF (*Pak Cyber Force*) consiguió publicar la página que se muestra en la Figura 3-5, reivindicando la libertad de Palestina(88).

Otro ejemplo de *defacing* lo protagonizó un grupo palestino conocido como *KDMSTeam* en octubre de 2013. Modificaron algunas páginas del conocido portal metasploit.com, que es el sitio web oficial del proyecto de código libre dedicado a analizar vulnerabilidades y ofrecer apoyo en el campo de la detección de intrusos y la seguridad de los sistemas. En la Figura 3-6 puede verse el resultado del ataque de los *hackers* palestinos(89).

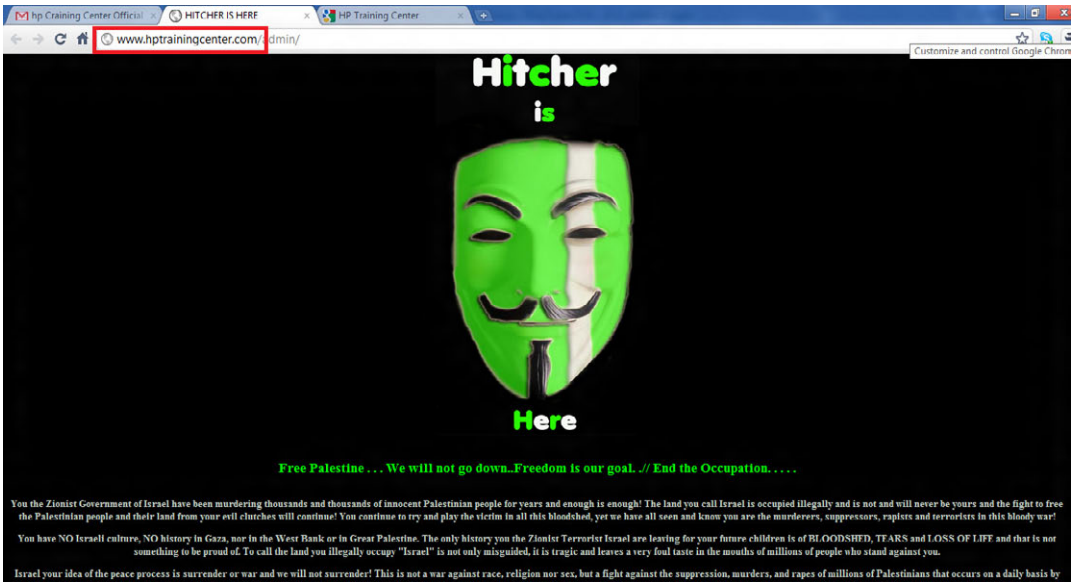


Figura 3-5: Ejemplo de *defacement*, realizado por Hitcher

En relación con el *defacement* por el objetivo de expresar ideas políticas, religiosas o sociales, aunque sin necesidad de modificación ilegal de datos en servidores web, se encuentran también los delitos de **apología del terrorismo y de la violencia**. Este es otro ejemplo de uso del ciberespacio como medio, y no como fin último u objeto del delito: se emplean modernas formas de comunicación y de publicidad de ideas radicales y violentas en blogs, foros, sitios web de medios de información y otros similares.

Figura 3-6: Otro ejemplo de *defacement*, realizado por el equipo KDMS

Otro caso de uso del ciberespacio como medio de comisión de actos ilícitos es la proliferación de situaciones de **acoso, injurias y amenazas** aprovechando medios telemáticos. En general, se habla de acoso en el ciberespacio para hacer referencia a cualquier conducta que implique una intención de amenazar, hostigar, avergonzar o dejar en ridículo a alguna persona, incluso llegando al chantaje en algunos casos. Los

medios utilizados pueden ser muy diversos, ya que puede emplearse mensajes de correo electrónico, mensajería instantánea o entre terminales móviles, publicación en blogs, foros y redes sociales, y sitios web de compartición de fotos o vídeos. El acoso implica una persistencia en las actuaciones con claras intenciones de perjudicar a la víctima, no incluyéndose las ocasiones puntuales y aisladas. La situación de la víctima es de miedo permanente, que se acentúa por la incapacidad de poner freno al acoso; por ejemplo, si son mensajes publicados en foros o blogs los que atacan a la víctima, ésta sabe que estarán permanentemente disponibles para que cualquiera los pueda leer, y habitualmente no hay un medio rápido de eliminarlos. Además existe temor a denunciarlo por las posibles represalias que se puedan tomar, lo que complica enormemente el problema.

Habitualmente se emplean términos que definen el tipo de acoso en particular, en función de quién realiza el acoso y qué tipo de persona es la víctima. Así, se denomina **ciberacoso** en general a las acciones en las que tanto el acosador como la víctima son adultos; cuando es un adulto quien acosa a un menor se habla de **ciberbullying**, y habitualmente tiene intenciones de tipo sexual. Un fenómeno que se extiende rápidamente es el acoso entre menores, denominado **grooming** y realizado normalmente en entornos escolares y entre menores de edades similares. No siempre es una sola persona la que realiza la agresión, pues puede haber otras que colaboren en mayor o menor medida, activa o pasivamente. La vigilancia en el uso que hacen los menores de las redes sociales es crítica para evitar situaciones peligrosas. En todos los casos las consecuencias pueden ser muy graves, habitualmente con secuelas de tipo psicológico, que pueden extenderse incluso al futuro, especialmente cuando son menores los que han sido víctimas del acoso. En algunos casos se llega al suicidio, como le ocurrió a la joven canadiense de 15 años Amanda Todd, quien tras tres años de acoso se suicidó, no sin antes publicar un video en YouTube denunciando su situación y anunciando su fatídico final(90).

También se llevan a cabo **delitos contra la propiedad intelectual**. Actualmente es relativamente fácil conseguir de forma gratuita en Internet material protegido por las leyes de los derechos de autor. No solo hay redes de intercambio de igual a igual (llamadas *peer to peer* o P2P), sino que numerosos sitios web ofrecen la descarga de material protegido o la visión en directo de películas. En fechas recientes se ha cerrado un sitio web de almacenamiento “en la nube”, *Hotfile*. Este sitio fue denunciado por la *Motion Picture Association of America* (MPAA, Asociación Cinematográfica de América), organización fundada en 1974 para proteger los intereses de los estudios de cine estadounidenses. La plataforma de almacenamiento deberá pagar 59 millones de euros por infringir las leyes de los derechos de autor. En nuestro país, el Grupo de Delitos Telemáticos de la Guardia Civil ha realizado recientemente detenciones y cierre de páginas web por vulnerar la propiedad intelectual e industrial(91).

Tampoco queda fuera del ciberespacio la **pornografía infantil**. Es éste un delito fuertemente penado y perseguido, a pesar de que no es fácil realizar seguimientos a los implicados. Los cibercriminales utilizan muchas herramientas que les proporcionan anonimato en Internet, y realizan gran parte de sus operaciones en la llamada web

profunda (que se estudiará con detalle en el punto 3.6). Este es el caso de una operación llevada a cabo por el Grupo de Delitos Telemáticos de la Guardia Civil recientemente, que ha traído como resultado la detención del responsable de difundir en Internet material relacionado con abuso sexual infantil. Las operaciones que llevaron al cibercriminal fueron complicadas precisamente por el uso de sistemas de anonimato y ocultación(92).

3.4 HERRAMIENTAS DEL CIBERCRIMEN Y EJEMPLOS DE USO

Se han descrito en el punto anterior muchos de los actos delictivos que se suelen realizar actualmente en el ciberespacio. Para llevarlos a cabo, los ciberdelincuentes necesitan por una parte una serie de herramientas, y por otra, ciertas técnicas de uso de tales herramientas y formas de proceder adecuadas a sus fines, que serán analizadas en el siguiente punto de este trabajo.

Respecto a las herramientas, algunas de ellas se han mencionado y comentado brevemente en el punto anterior; en éste se profundizará en este aspecto del cibercrimen, describiéndose con más detalles tanto las que han aparecido anteriormente como otras, e ilustrando en algunos casos las explicaciones con casos reales de delitos y ataques realizados y conocidos públicamente. No se pretende tratar de forma completa y exhaustiva todas las herramientas que usan los cibercriminales, pues ello puede ser objeto de estudio de otro proyecto independiente, sino dar una idea general de las mismas.

En este texto se ha estado usando profusamente la palabra *malware*, como sinónimo de software maligno o código dañino. Hay una gran cantidad de software que puede englobarse en esta categoría, con diferentes objetivos, arquitecturas internas, técnicas de propagación e infección y formas de operación. Es frecuente en el lenguaje común hablar de virus, troyanos y gusanos. Cada uno de estos términos indica una forma de proceder del *malware* en cuestión. Realmente no hay ni siquiera consenso en cuanto a algunas particularidades de las definiciones de cierto *malware*, aunque sí hay algunos rasgos generales que se comentarán aquí. En la literatura especializada también se puede encontrar el término ***crimeware*** para referirse al *malware* utilizado con fines delictivos en general aunque a veces se encuentran versiones que indican que este término solo se refiere a código que tiene objetivos económicos.

El término más empleado cuando se quiere hacer referencia a algún software dañino o no deseado es “virus”. De manera general, se puede definir al **virus informático** como cualquier *malware* que se introduce en un sistema sin intención por parte del usuario o administrador, modificando algún o algunos archivos o bien los sectores de arranque de los discos. Este software introducido en el sistema realiza a lo largo del tiempo una labor de infección: habitualmente, al lanzarse posteriormente otros archivos ejecutables, éstos quedan infectados por el propio virus, y de esta manera el virus se va propagando dentro del sistema. Además de esta acción de copia suelen realizar alguna otra actividad maligna adicional, como puede ser la destrucción de archivos o de discos enteros, el robo de información, la inhabilitación de ciertas aplicaciones legítimas (como por

ejemplo los antivirus) o la ralentización del equipo. Otros virus simplemente tienen la intención de molestar al usuario y demostrar que han podido infectar su sistema (como ejemplo se puede citar el virus denominado W32/Gruel, que afectaba a sistemas Windows 9.x/ME(93)) y en otros casos la finalidad es mostrar insistentemente algún tipo de publicidad al usuario, ya sea cuando el usuario ejecuta algún programa concreto, o bien redirigiendo su navegador web a ciertas páginas; en estos casos se habla de ***adware***[41]. Este término se aplica tanto al software que se instala de manera no deseada por el usuario como al que lo hace con el consentimiento del mismo; en estos últimos casos, suele venir incluido en aplicaciones que son gratuitas y se financian con los anuncios. Habitualmente se observa que el software no realiza modificaciones importantes o peligrosas en el sistema, siendo la molestia al usuario el principal daño causado. En algunas ocasiones se puede realizar algún tipo de pago para que desaparezcan los anuncios(94).

Otro término relacionado es "**troyano**" o "caballo de Troya", que hace referencia a un tipo de código dañino que, disfrazado de aplicación útil, realiza alguna acción no consentida en el equipo infectado, entre las cuales se cuentan robar información o permitir el acceso remoto no consentido por el dueño del equipo, por ejemplo. Los troyanos, por definición, no se auto-propagan.

También se habla a menudo de "**gusanos**"; es el software cuya principal función es propagarse, por cualquier medio (enviando copias de sí mismo por correo electrónico, copiándose a unidades de almacenamiento en red o a unidades de disco locales externas tipo USB, aprovechando mecanismos de procedimientos de llamadas remotas en otros equipos, etc.). Los gusanos, de por sí, no tienen intención maligna adicional, aunque el daño que provocan es el uso de recursos (de almacenamiento y de comunicaciones) en su propio proceso de propagación. Un ejemplo de este caso fue una denegación de servicio masiva ocurrida en enero de 2003. Un gusano llamado *Slammer* surgió en algún lugar del este de Asia, y se propagó en cuestión de minutos por todo el mundo. Cada 8,5 segundos el número de equipos infectados se dobló, infectando a varios miles de equipos en Internet en un tiempo muy corto: en 10 minutos se produjo el 90% de las infecciones. El gusano no modificaba ningún archivo del disco de los sistemas infectados, ya que simplemente aprovechaba una vulnerabilidad (desbordamiento de *buffer*) del software SQL Server de Microsoft para ejecutar código remotamente y propagarse. El funcionamiento del gusano hacía que éste fuera escaneando equipos vulnerables continuamente; de hecho, alcanzó su tasa máxima de escaneo en unos 3 minutos, llegando a unos 55 millones de escaneos por segundo. A pesar de que el gusano no contenía ningún *malware* aparte del propio proceso de infección, el volumen de tráfico que suponía el funcionamiento del gusano[42] provocó

[41] *Adware* viene del inglés *ad(vertisement)* = anuncio.

[42] Algunos *routers* no pudieron procesar todos los paquetes que les llegaban y dejaron de funcionar; los *routers* cercanos tuvieron que reconstruir sus tablas de direccionamiento, colapsándose a su vez multitud de enlaces y provocando que más *routers* cesaran en su funcionamiento.

una denegación de servicio a escala masiva: miles de cajeros automáticos se desconectaron en EEUU, se cancelaron muchos vuelos y el servicio de emergencia de EEUU (el llamado "911", equivalente al "112" en Europa) se vio también afectado(95).

Existen también las llamadas "**puertas traseras**" o *back doors* que ofrecen la posibilidad de acceder, por medios no documentados ni solicitados, al control de cierto software o de la máquina que lo alberga, sin levantar sospechas y sin detección cuando se realiza ese control oculto; habitualmente se realiza por parte del propio programador del software en cuestión, para tener control remoto de ciertas funciones sin necesitar aviso previo ni permiso del usuario. En otras ocasiones las puertas traseras se instalan en los sistemas por medio de troyanos.

Las "**bombas lógicas**", por otra parte, son un tipo de *malware* que realizan alguna acción dañina únicamente cuando se cumple una condición o una serie de condiciones. Si la condición es que llegue una determinada fecha u hora, se denomina "bomba de tiempo". Un ejemplo es el "virus de Chernobyl", también conocido como CIH (por las iniciales de su autor, Chen Ing-Hou), que se activaba cada 26 de abril (aniversario del accidente en la central nuclear ucraniana), borrando el disco duro e, incluso en algunas variantes, parte de la BIOS (96)(97).

Es importante considerar que las definiciones anteriores, y en general cualquier tipo de clasificación similar, no implican que algún *malware* concreto deba ser considerado obligatoriamente solo como virus o solo como troyano; en muchas ocasiones se realizan por un solo *malware* varias de las funciones señaladas anteriormente por las diferentes categorías de código dañino (incluso se considera en muchos entornos que los troyanos, gusanos, etc. son tipos particulares de virus). En cualquier caso, como se ha comentado anteriormente, en este texto se dan solo algunas de las características generales, pues el objetivo último es entender cuáles son las herramientas con las que se realizan muchas de las acciones cibercriminales hoy en día.

Las acciones perniciosas que realizan los distintos tipos de *malware* antes comentados son muy variadas. Algunas son realmente peligrosas, como el borrado de información o la denegación de uso de equipos informáticos debido al alto consumo de recursos. En otros casos, lo que hace el *malware* es capturar las teclas que pulsa el usuario en su teclado, para posteriormente enviar las secuencias al *hacker* o ciberdelincuente que explota la herramienta. A este tipo de *malware* se le llama ***keylogger***; habitualmente se utiliza para capturar credenciales de acceso a sistemas informáticos o a sitios web que van a ser objeto de ataques posteriores. De nuevo hay que indicar que los conceptos se mezclan, de tal manera que un *keylogger* puede ir oculto en un programa de uso general y aparentemente inocuo, en forma de troyano. Los *keyloggers* se utilizaron mucho anteriormente, aunque no siempre conseguían su objetivo. Considérese, por ejemplo, el caso de acceso a algún sistema remoto a través de un interfaz web. Si el usuario utiliza la técnica de copiar y pegar las credenciales (ya sea con ratón o con teclado), el *keylogger* no podrá capturar la información deseada; tampoco podrá capturar la información indicada en listas desplegables, en las que el usuario elige con el ratón una opción de entre varias que se le ofrecen. Por ese motivo, y unido a la utilización cada vez mayor de

interfaces web, los *keyloggers* han dado paso a otro tipo de *malware* llamado ***form grabber***. Este nuevo *malware* captura la información que los navegadores envían al servidor web cuando el usuario rellena algún formulario y pulsa el botón "enviar" o "ir" correspondiente. Hay varias maneras de conseguirlo, una de las cuales es instalar en el navegador del usuario alguna extensión o barra de herramientas malignas que disfracen sus verdaderas intenciones bajo la apariencia de alguna utilidad (se podría considerar un troyano). En otras ocasiones el *malware* intercepta alguna llamada dentro del sistema relacionada con el envío de información HTTP[43]. La ventaja del uso de *form grabbers* es que el ciberdelincuente recibe la información deseada y de manera escueta (dirección IP y URL del servidor web al que se accede, usuario, contraseña y resto de datos del formulario; con los *keyloggers* recibiría muchísimas pulsaciones del teclado procedentes del uso normal del equipo, y tendría que buscar entre ellas cuáles responden a un acceso a algún tipo de servidor); la desventaja es que sólo sirve para accesos vía web, aunque cada vez se utiliza más este interfaz para acceso a sistemas importantes. Un ejemplo de *form grabber* es el troyano llamado Nethell/Limbo Trojan(98).

Hay otros tipos de *malware* que, siguiendo con la dinámica anterior de evolución de obtención ilícita de credenciales de acceso, capturan las zonas de la pantalla donde el usuario hace clic con el ratón. Este software, más elaborado, se utiliza para robar información de acceso en webs que utilizan teclados en pantalla, como la indicada en la Figura 3-7.

Figura 3-7: Acceso a un banco por web, con teclado en pantalla

Además de todos los tipos anteriormente expuestos, se han acuñado algunos términos para referirse a cierto software malicioso con intenciones concretas. Así, se denomina

[43] HTTP significa *HyperText Transfer Protocol*, protocolo de transferencia de hipertexto. Es el protocolo usado en la interacción entre navegadores y servidores web, entre otros usos. Algunos *form grabbers* interceptan por ejemplo la llamada *HttpSendRequest* en Windows

spyware al que tiene como intención, de forma general, robar información de equipos de usuario. Los datos robados pueden ser muchos y muy variados: direcciones IP, nombres de equipo, información de contactos (correos electrónicos, números de teléfono, etc.), credenciales de acceso, listado de ficheros en medios de almacenamiento, procesos en ejecución en el sistema infectado, historial de navegación web, pautas de uso del equipo, ficheros descargados durante la navegación por Internet, etc. La funcionalidad es más amplia que la de los *keyloggers* o *form grabbers*, aunque se puede combinar con éstos en muchos casos. El *spyware* se puede introducir en un sistema en forma de troyano. Un ejemplo de *spyware* es el llamado Sinowal.CR(99); entre otras cosas, captura la comunicación entre los navegadores del equipo infectado y los servidores de Internet. Curiosamente, llega a borrar las *cookies* de los navegadores para obligar al usuario a volver a teclear las credenciales que se hubieran introducido antes de la instalación del *malware*, y así tener acceso a más datos. Otro ejemplo muy conocido y más elaborado de *spyware* es el denominado Rona.A(100), utilizado para realizar espionaje industrial a una empresa de Israel en 2005. Este software registraba entre otras cosas los procesos activos del sistema víctima y la disponibilidad de conexión a Internet, y además se conectaba a un determinado servidor para actualizarse periódicamente, recibir archivos de configuración, recibir órdenes de actuación, subir documentos previamente seleccionados por el delincuente que lo estuviera controlando, enviar información de los sitios web visitados desde el equipo infectado, enviar pulsaciones de tecla guardadas (hacía por tanto funciones de *keylogger*) o enviar capturas de pantalla, no solo estáticas: incluso enviaba vídeos con la actividad del equipo en cuestión. Como último ejemplo puede mencionarse el troyano Hesperos (Win32/Spy.Hesperbot), descubierto en verano de 2013 y diseñado para realizar fraudes bancarios. Este software es capaz de capturar la pantalla del ordenador infectado y de realizar vídeos durante su uso; también hace un inventario de las *smart-cards* presentes en el sistema. Asimismo realiza funciones de *proxy* en el ordenador infectado, interceptando las comunicaciones con entidades bancarias (usando la técnica conocida como "hombre en el medio" o, en inglés, "*Man in the middle*"). Proporciona su propio certificado SSL[44] autofirmado, y para evitar que el usuario reciba un aviso de certificado no válido modifica la configuración del navegador. Tiene funciones de captura de pulsaciones de tecla o *keylogger* y permite que el escritorio del equipo de la víctima sea controlado remotamente mediante el protocolo VNC[45]. Para evitar estas amenazas algunos usuarios configuran sus accesos a las entidades bancarias para que utilicen autenticación en 2 pasos, de tal manera que al acceder a la web del banco, éste envía al teléfono móvil del usuario una contraseña de un solo uso (OTP, *One Time Password*, también conocida en este caso como mTANs, *Mobile Transaction Authentication Number*). El troyano Hesperos tiene un componente móvil para capturar estas contraseñas temporales, con versiones para varios sistemas operativos móviles

[44]SSL, S*ecure Socket Layer*, es un protocolo para comunicación segura utilizando certificados digitales.

[45]*Virtual Network Computing*: es un software utilizado para controlar remotamente el escritorio de otro equipo.

(Symbian, Blackberry y Android). Una vez el móvil recibe la contraseña del banco, el *malware* la reenvía al móvil del atacante(101)(102)(103). Como se puede ver, la sofisticación del software dañino es a veces muy elevada.

Otro término que se ha venido utilizando es el de ***ransomware***. Ya se habló de él en el punto 3.3 (ver página 60) y se indicó allí que es un tipo de *malware* que secuestra un equipo, dejándolo inutilizable hasta que la víctima pague un rescate al ciberdelincuente, cometiéndose por tanto un delito de extorsión. Este tipo de *malware* puede entrar en los sistemas de varias maneras, por ejemplo como troyanos disfrazados en ejecutables aparentemente inofensivos. Este tipo de chantajes suele tener un beneficio económico elevado para los cibercriminales; de hecho, según algunos de los últimos informes de la empresa McAfee, se ha visto un incremento notable en el número de muestras de *ransomware* en el año 2013 respecto al año anterior(104). Algunos ejemplos de este software maligno utilizan técnicas tan sencillas que se implementan en *javascript* dentro de algunos navegadores, posibilitando que llegue incluso a plataformas informáticas que tradicionalmente han sido menos atacadas, como es el caso de equipos de usuario de Apple ejecutando el sistema operativo OS X. En verano de 2013 aparecía en multitud de medios de información especializados la noticia de que los usuarios del navegador Safari estaban recibiendo mensajes indicando que sus equipos habían sido utilizados para realizar acciones ilícitas, visitar páginas pornográficas o violar leyes de derechos de autor. Tales mensajes decían proceder del FBI norteamericano, y se exigía a los usuarios el pago de un rescate para volver a obtener el control del navegador(105). Por suerte, y debido a la tecnología empleada, bastaba con reiniciar la configuración general del navegador para eliminar el *malware*, pero este caso proporciona una idea de qué tipo de argucias utilizan los cibercriminales para obtener dinero.

Precisamente el uso de mensajes que dicen proceder de algún departamento policial es una tendencia del *ransomware* desde el año 2011. En España fue famoso el llamado “virus de la Policía”, que se hacía pasar por la Policía Nacional para pedir un rescate de 100€(106); de igual manera ocurría en otros países, como en Alemania con la Policía Federal Criminal (BKA, *Bundeskriminalamt*)(107). En ambos casos el equipo quedaba bloqueado hasta que el usuario pagara el rescate, aunque se podía eliminar el *malware* pasando un antivirus que se iniciara desde un CD o memoria USB. Los mensajes que suelen aparecer en los equipos de las víctimas son bastante reales, pues los cibercriminales llegan a utilizar los escudos y símbolos oficiales (ver Figura 3-8).

Figura 3-8: Infección por el virus de la Policía

Si en el caso del virus de la Policía el equipo infectado quedaba bloqueado hasta que se produjera el pago del rescate o fuera eliminado el virus, en otros casos el *ransomware* permite seguir utilizando el equipo pero en otras circunstancias. El caso comentado anteriormente de *CryptoLocke r*es muy típico, pues este software cifra todos los archivos de datos del usuario (más de 70 tipos de archivo, entre otros documentos de texto, hojas de cálculo, imágenes y archivos PDF) y pide una cantidad de dinero para descifrarlos. Lo grave de esta operación es que el cifrado se realiza con técnicas de clave pública, estando la clave privada en el servidor del ciberdelincuente. En el caso de *CryptoLocker* cuando un equipo llega a ser infectado, contacta con un servidor controlado por el ciberdelincuente. Entonces, el servidor genera un par de claves (pública y privada, de 2048 bits); la clave privada se queda en el servidor, y la pública se envía al equipo infectado; en éste se genera a su vez otra clave para cifrar, mediante AES y por tanto de manera muy rápida, multitud de archivos de los discos fijos, extraíbles y de red. La clave AES se cifra a continuación con la clave pública del servidor y se guarda en éste. El sistema empleado hace prácticamente imposible recuperar los archivos cifrados si no se paga el rescate o se recupera una copia de seguridad. Como es habitual en este tipo de extorsiones, se le da un plazo a la víctima para pagar (3 días), tras el cual la clave privada se borrará del servidor. Entre las víctimas de este virus está la policía local de Swansea, en Massachusetts (E.E.U.U.), que tuvo que pagar 750$ para volver a tener acceso a sus archivos(108). En los primeros días de 2014 se ha detectado que CryptoLocker ha evolucionado para poder propagarse automáticamente, sin ayuda externa ni intervención del usuario, convirtiéndose así en un gusano(109).

Una variante del *ransomware* es el ***scareware***, comentado en el punto 3.3 (página 57); en este caso se avisa a las víctimas de los equipos infectados de que éstos tienen un

virus, aunque tal extremo no es real; en cualquier caso, invitan al usuario a que adquiera un antivirus que tampoco es real, y que a su vez se engloba en la categoría del denominado ***rogue software***, literalmente "software pícaro" o software falso.

Todos los tipos de software maliciosos comentados hasta ahora son susceptibles de ser detectados por herramientas adecuadas (antivirus principalmente). Sin embargo, hay otro tipo de software complementario que les permiten instalarse y pasar inadvertidos a los antivirus y que reciben el nombre genérico de ***rootkits***[46]. Habitualmente los *rootkits* se instalan en los equipos en algún nivel que le permita tener un control elevado del mismo, de forma que pueden interceptar llamadas al sistema de diversas aplicaciones, entre ellas las de los propios antivirus. Es habitual que los *rootkits* se instalen en el núcleo del sistema operativo, o bien que modifiquen algunas de las librerías básicas del sistema; a partir de ahí son capaces de esconder los procesos malignos de manera que no aparezcan en la lista de procesos del sistema, o de impedir por completo que los ficheros donde están escondidos los virus puedan ser accedidos por herramientas del propio sistema o del espacio de usuario. Su detección y eliminación son por tanto difíciles.

Según un informe del grupo de trabajo anti-*phishing* (APWG, *Anti-Phishing Working Group*) titulado "*Phishing Activity Trends Report – 2nd Quarter 2013*" y publicado en noviembre de 2013(110), el tipo de *malware* que más infecciones realiza es la categoría de troyanos, con casi un 80%, seguido de gusanos con casi un 7% y virus con un 6%. La conocida empresa PandaLabs, siempre según el mencionado informe, considera que casi un 33% de los ordenadores de todo el mundo estaba infectado con algún tipo de código dañino en el segundo cuatrimestre de 2013; en China ese porcentaje alcanzaba la mitad de los equipos informáticos. En Turquía la tasa era de casi un 44%, y varios países de América Latina tenían porcentajes muy parecidos (Perú: 42%; Bolivia: 41'7%; Ecuador: 41%; Argentina: 39%). Rusia también presentaba una tasa alta de infección con un 41%.

3.5 TÉCNICAS Y PROCEDIMIENTOS DE INFECCIÓN Y ATAQUE

Una vez conocidos algunos de los tipos de código dañino que pueden encontrarse en el ciberespacio, cabe preguntarse cómo pueden llegar a infectar a los equipos de las víctimas, o dicho de otra manera, qué técnicas utilizan los ciberdelincuentes para utilizar las herramientas ya vistas, hacerlas llegar a los usuarios finales y así poder perpetrar de manera práctica sus acciones ilícitas. En este sentido, debe recordarse que hay delitos que no requieren necesariamente la ejecución de código dañino, y otros sí lo requieren.

3.5.1. PHISHING, SPAM

Dentro de los delitos que no requieren la ejecución de código dañino está el robo de información, comentado en el punto 3.3. Se indicó que las víctimas no son conscientes

[46] Del inglés *root* = raíz, aunque también hace referencia al nombre de usuario privilegiado en sistemas Unix y derivados.

de que están facilitando información privilegiada a los delincuentes, y que una de las maneras más habituales de conseguir el robo es mediante el llamado *phishing*, consistente en configurar y publicar un servidor web con páginas idénticas a las del servicio (habitualmente de tipo bancario) del cual se quieren conocer las credenciales de las víctimas. De entre las distintas formas de atraer a los usuarios a esas copias falsas de las páginas web, una es mediante el envío de correos masivos engañosos, es decir, mediante la técnica del *spam*. Ya se indicó en la página 62 que es habitual utilizar el *spam* para conseguir timos como los de las cartas nigerianas y los de las loterías, pero también es la manera más usada para provocar el robo de información por *phishing*. Normalmente los servidores que albergan páginas destinadas al robo de información no están operativos durante mucho tiempo, pues existen muchas organizaciones y empresas de seguridad que realizan seguimientos en tiempo real y denuncian persiguen a tales páginas. De acuerdo con un documento del APWG publicado en otoño de 2013 titulado "*Global Phishing Survey 1H2013: Trends and Domain Name Use*"(111), durante la primera mitad de ese año la media de tiempo que estuvieron operativos los servidores falsos fue de 44 horas y 39 minutos, más que las 26 horas que se midieron en la segunda mitad de 2012. Estas medidas son importantes, pues se considera que el primer día que se produce un ataque de *phishing* es el más lucrativo, y luego los ciberdelincuentes tienen que eliminar el servidor, tras ser descubiertos. Un aumento del tiempo de servicio puede indicar un mayor éxito de los ciberdelincuentes. Otro informe del mismo grupo ya mencionado anteriormente ("*Phishing Activity Trends Report – 2nd Quarter 2013*"(110)) indicaba que los países que albergaron la mayor parte de los servidores falsos en el segundo cuatrimestre de 2013 eran E.E.U.U., Rusia, Alemania y Canadá; Hong Kong tenía un porcentaje notable en abril, pero en mayo y junio desapareció, subiendo bastante el *phishing* realizado con servidores en Kazajistán. El informe de Symantec ya mencionado anteriormente(78) indica que en lo que se refiere a la actividad de *phishing* detectada en 2012, los principales países a los que se dirigían las campañas eran Países Bajos, Sudáfrica, Reino Unido, Dinamarca y China. En cuanto al *spam* en general, los principales países a los que iban dirigidos los mensajes de correo electrónico en 2012 fueron Arabia Saudí, Bulgaria, Chile, Hungría y China. El volumen de *spam* diario en 2012 se estimó en 30.000 millones de mensajes. Los asuntos de los que trataban los mensajes eran principalmente productos farmacéuticos y citas para adultos. En cualquier caso, los ciberdelincuentes van adaptando continuamente la temática, las características y los destinatarios de los mensajes.

En muchas ocasiones no es necesario engañar a las víctimas mediante envío de correos electrónicos con direcciones falsas de servidores bancarios, pues se realizan ataques más sofisticados. Por ejemplo, es posible modificar la configuración del equipo de la víctima o de su *router* de acceso a Internet de tal manera que, cuando intente navegar a una página web de alguna entidad bancaria, se le redirija a un servidor falso que robará las contraseñas. Estos ataques suelen hacerse en general a alguna parte del sistema de resolución de nombres de dominio (DNS, *Domain Name System*), de forma que la víctima no es consciente de la redirección, pues no ha tenido que seguir ningún enlace que se le haya enviado en correos electrónicos de *spam.* A esta técnica se le denomina ***pharming***.

El *phishing* por *spam* mediante correo electrónico admite algunas variantes, como por ejemplo el envío de mensajes cortos a móviles (SMS) invitando a visitar alguna página web desde el propio terminal; en este caso se habla de ***smishing*** (contracción de SMS y *phishing*). También se configuran servidores de voz sobre IP (VoIP) con locuciones similares a las que se emplean en entidades bancarias para que, tras invitar a las víctimas a llamar, éstas proporcionen sus claves a través del teléfono, aprovechando que este tipo de comunicación se considera seguro en general por parte de los usuarios de servicios bancarios. Esta técnica se denomina ***vishing*** (VoIP *phishing*). Una variante mucho más evolucionada, aunque no demasiado habitual, es el llamado *hishing* (*hardware phishing*), consistente en fabricar equipos (teléfonos móviles, reproductores multimedia y similares) que contienen algún tipo de código dañino o puerta trasera. En relación con este tema, recientemente ha habido rumores de que ciertos productos de fabricantes muy conocidos internacionalmente (Cisco, Dell, Juniper y Huawei entre otros) tenían vulnerabilidades que son aprovechadas por la agencia norteamericana NSA (*National Security Agency*, Agencia de Seguridad Nacional)(112). No está claro si esta circunstancia era conocida por los propios fabricantes o bien un equipo especializado de la NSA denominado ANT ha logrado encontrar agujeros de seguridad en ellos. La compañía china Huawei ha tenido que desmentir recientemente que sus productos tengan fallos de seguridad voluntariamente implementados; es irónico que a esta compañía se le acuse de actuar bajo órdenes de la NSA, cuando precisamente por sospechas relacionadas con la seguridad había perdido previamente contratos con organismos oficiales de E.E.U.U. tras haber sido relacionada con las actividades militares chinas(113).

En las técnicas de *phishing* los cibercriminales se valen de argucias varias, algunas basadas en la falta de atención de los usuarios. Por ejemplo, se puede pensar en un mensaje de correo de *spam* que indique que el servicio de correo electrónico de Google, Gmail, quiere confirmar la contraseña para evitar acciones de delincuentes y por su seguridad. Se podría redirigir a la víctima a un sitio que supuestamente sería de Google, pero en cuya URL se haya sustituido la letra minúscula “l” por el número “1”, quedando la dirección gmai1.com en vez de gmail.com. Este detalle puede pasar inadvertido para la mayor parte de los usuarios. Al acceder a la dirección fraudulenta podría aparecer un aviso de seguridad en el navegador del usuario (si está bien configurado), indicando que hay un problema con el certificado del servidor. Por la experiencia acumulada se sabe que la mayor parte de los usuarios obvian el aviso de seguridad, aceptando la conexión. Esto es debido a la falta de conocimientos técnicos, circunstancia que también saben aprovechar los ciberdelincuentes. En otras ocasiones no aparece el aviso de seguridad; puede ser porque el equipo de la víctima haya sido manipulado con algún código dañino previo, modificando la configuración del navegador para que no muestre avisos de seguridad[47], pero también por presentarse un certificado válido, ya que ha habido casos de robos de certificados de firma de código a grandes organizaciones, usándose en

[47] Se cita un ejemplo de troyano que modifica la configuración del navegador para que no informe de un certificado no válido en la página 63.

varias ocasiones para propagar *malware* en nombre de Microsoft, Adobe y Opera(114)(115)(116).

De los ejemplos citados se puede intuir que el hecho de que el *phishing* y el *spam* tengan éxito es debido a un factor que se menciona habitualmente en los foros dedicados a la seguridad informática y de la información: el elemento más débil de la cadena de seguridad es el humano. Se refiere esta expresión principalmente al elemento humano como usuario final de los sistemas, aunque también se podría hablar del elemento humano en cuanto a administradores y gestores de los mismos, ya que si éstos son víctimas de engaños, los delincuentes pueden lograr acceso a servidores, sistemas o sitios web desde los cuales se pueden lanzar posteriores ataques, llegando más lejos que si la víctima es un usuario final. En cualquiera de los casos los cibercriminales hacen uso de la llamada "**ingeniería social**", es decir, el conjunto de técnicas de manipulación y engaño de las víctimas para conseguir los objetivos delictivos. En este sentido se ha observado un cambio de tendencia en los comportamientos de los ciberdelincuentes en los últimos años, pues la enorme expansión en el uso de las redes sociales les ha dado nuevas oportunidades. En estos entornos se observa una serie de características y de pautas de comportamiento de los usuarios que permiten que se cometan engaños con mayor facilidad y expansión. Una de ellas es el efecto llamado "demostración social" o "*social proof*" consistente en que el ser humano suele hacer lo mismo que hace el resto de la gente, encontrando internamente un cierto grado de aprobación (quizá por falta de seguridad en sí mismo) al actuar de la misma manera que como lo hacen los demás de su entorno. Esta circunstancia es muy conocida en las técnicas de mercadotecnia (marketing), y aplicado a las redes sociales implica que los usuarios emularán las acciones de sus amigos o contactos (visitarán las mismas páginas, les gustarán las mismas cosas), especialmente si son cercanos o de confianza. Si a este comportamiento se le une el hecho de que la esencia de las redes sociales es la compartición (de información personal, actividades, aficiones, gustos, etc.) se llega a una situación ideal para los ciberdelincuentes, que encuentran un terreno muy útil tanto para propagar código dañino o enlaces como para encontrar información personal, algo que puede ser utilizado para realizar ataques concretos muy efectivos (véase la página 86 en la que se habla de ataques dirigidos). En algunos casos incluso se llega a secuestrar cuentas de usuarios en redes sociales para realizar técnicas de *spam* con las cuentas, o bien para hacer publicaciones que contienen enlaces a sitios peligrosos(117). Por estos motivos ha habido una expansión (en algunos casos un desplazamiento) de las amenazas por los canales tradicionales a estos nuevos ámbitos, y de hecho algunos informes indican que se ha visto últimamente una reducción en los ataques por *phishing* y *spam*(78).

De igual forma que se observa una tendencia a utilizar y ocupar las redes sociales por parte de los cibercriminales, se está viendo el aprovechamiento de nuevas plataformas, como los dispositivos móviles (teléfonos móviles y tabletas principalmente). Según el informe de la empresa de seguridad Symantec de 2013 de la referencia (78), ha habido un incremento de un 58% en el *malware* de dispositivos móviles en el año 2012 respecto a 2011, lo cual no es de extrañar teniendo en cuenta que se produjo un aumento de un 32% en el número de vulnerabilidades en sistemas operativos de móviles. En el último

informe disponible de amenazas de McAfee, correspondiente al tercer trimestre de 2013, esta compañía de seguridad había acumulado un total de 680.000 muestras de *malware* solo para el sistema operativo Android (el más atacado, por otra parte)(118). El primer troyano para este sistema operativo se descubrió en 2010; llamado *Trojan-SMS.AndroidOS.FakePlayer.a*, se disfrazaba bajo una aplicación reproductora de medios y enviaba SMS sin permiso del usuario a servicios de tarificación especial que pertenecían a los delincuentes (puede consultarse al respecto un análisis en profundidad del troyano en el documento indicado en la referencia(119)).

3.5.2. SKIMMING, CARDING Y TÉCNICAS ASOCIADAS

Otro caso de ciberdelito que no requiere infección por *malware* es el *carding*, consistente, como se comentó en la página 57, en utilizar fraudulentamente tarjetas de crédito o débito ajenas. En este punto dedicado a las técnicas usadas por los ciberdelincuentes, se hablará de algunas formas de obtener datos de tarjetas de crédito o débito, denominadas en general *skimming*. En general, los datos que se necesitan de una tarjeta de crédito o débito son los almacenados en su banda magnética, y también es interesante obtener el código de seguridad (código PIN). Una vez obtenidos los datos, los delincuentes pueden utilizarlos para efectuar transferencias o extracciones de dinero, para realizar compras directamente, o bien para venderlos posteriormente en foros especializados del cibercrimen. Para conseguirlos datos de las tarjetas los ciberdelincuentes suelen instalar de algún tipo de equipamiento (llamado en general *skimmer*) en lugares frecuentados por usuarios de las mencionadas tarjetas. Los lugares más habituales son cajeros electrónicos, aunque también se han descubierto muchos equipos en multitud de negocios (gasolineras, tiendas minoristas, etc.).

El equipamiento más habitual consiste en un lector de tarjetas con banda magnética. Este elemento se puede conseguir fácilmente y a un precio bastante bajo. Habitualmente se eligen lectores que se parecen mucho en el color y en el diseño a los originales del sitio donde se van a colocar. Como ejemplo, obsérvese la Figura 3-9, en la cual aparece en la parte izquierda el lector real de un cajero y en la derecha otro que se instaló posteriormente por unos delincuentes.

Figura 3-9: Lector real de un cajero (izquierda) y lector instalado por ciberdelincuentes (derecha)

Con un lector como el indicado el delincuente ya puede tener los datos de la numeración de la tarjeta, pero faltaría conocer el PIN. Esto no suele ser un problema, pues de manera adicional al lector de tarjetas se suele instalar alguna cámara que graba las pulsaciones del teclado, de forma que cuando el usuario teclea el PIN de su tarjeta, las imágenes quedan grabadas. El lector de la Figura 3-9 es tan sofisticado que dispone de su propia cámara; puede observarse con más detalle en la Figura 3-10, donde se ve el orificio (señalado por una flecha) por el cual la cámara graba las operaciones en el teclado del cajero.

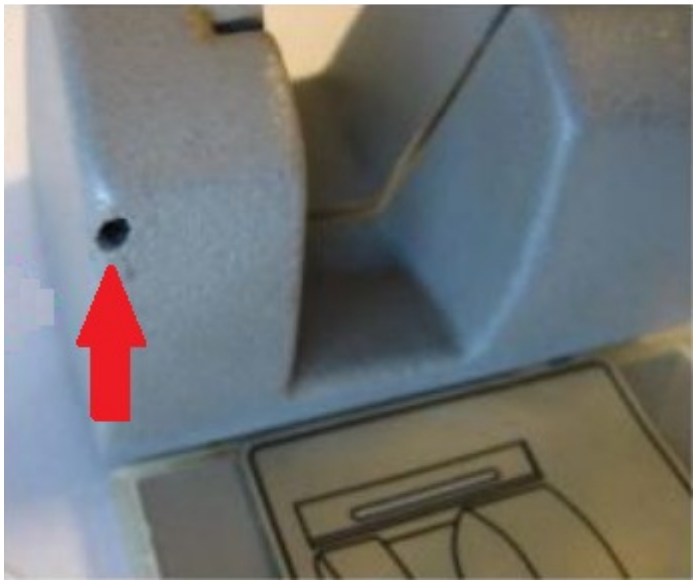


Figura 3-10: Detalle de la cámara en el lector de tarjetas

En algunas ocasiones la cámara se instala en algún lugar a mayor altura y apuntando al teclado del cajero automático, simulando ser parte de la infraestructura de vigilancia y seguridad de la entidad bancaria. En otras se monta una cámara oculta tras un espejo que supuestamente permite a los usuarios del cajero comprobar si alguien les está

observando mientras realizan sus operaciones, cuando en realidad es el delincuente el que lo hace con el dispositivo dentro del espejo. En la Figura 3-11 puede verse un ejemplo, y en la Figura 3-12 se ve el detalle del agujero por donde se graba la operación con el teclado del cajero. El usuario realizará sus operaciones tranquilamente, pensando incluso que la entidad bancaria está poniendo medios adicionales a su alcance para aumentar su seguridad.

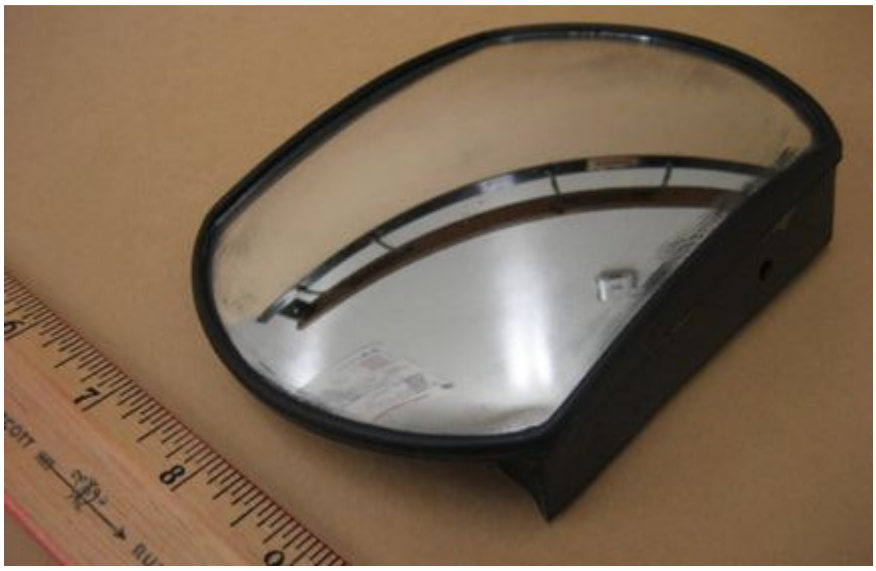


Figura 3-11: Espejo para que el usuario del cajero observe si alguien le vigila

Figura 3-12: Detalle del orificio por donde se graba la introducción del PIN

A veces se utilizan medios técnicos algo más artesanales, aunque la habilidad de los delincuentes consigue que no se note ninguna manipulación. En la Figura 3-13 se muestra un cajero aparentemente normal, tal como se lo encontraría cualquier usuario. Sin embargo ha sido objeto de manipulación, como se comprueba en la Figura 3-14; aquí se puede apreciar que es un teléfono móvil, situado convenientemente para que

enfoque al teclado, el que realiza las capturas de las imágenes. La ventaja en este caso es que el propio móvil, si ha sido programado convenientemente, puede enviar inmediatamente las imágenes por correo electrónico, o guardándolas en algún servidor FTP, o de la manera que el delincuente considere más conveniente.

Figura 3-13: Cajero automático aparentemente sin manipular

Figura 3-14: Detalle de un dispositivo móvil para grabación del PIN

Otra posibilidad usada por los ciberdelincuentes permite no tener que desmontar el cajero; muchos de ellos se encuentran en habitáculos que están normalmente cerrados, y para poder entrar hay que pasar la tarjeta en un lector que se encuentra fuera del mismo, tras lo cual se abre la puerta. Se han visto casos en los que se ha desmontado el lector exterior, sustituyéndolo por otro propiedad de los delincuentes (similar al de la Figura 3-15), el cual se conecta al mecanismo de apertura de la puerta. Dentro se ha

instalado alguna cámara en algún lugar estratégico para grabar la introducción del PIN por parte de las víctimas. De esta manera el cajero no se manipula, y el personal de seguridad o de operaciones del banco no descubrirá el fraude fácilmente.

Figura 3-15: Lector externo de tarjetas para acceso al cajero automático

Aunque no es del todo habitual, también se han dado casos en los que los delincuentes han montado una estructura completa delante del cajero automático original; esto ocurrió, por ejemplo, en Brasil, donde en octubre de 2013 se descubrió que alguien había instalado un cajero falso encima de uno verdadero. Un cliente quiso realizar una operación y el cajero le indicó que no estaba disponible, pero para entonces ya se había capturado la información de su tarjeta. En el video de YouTube indicado en la referencia (120) puede verse cómo se desmonta el cajero falso y su contenido (aparentemente un ordenador portátil, algunas baterías y un teclado donde las víctimas teclearían los códigos que se iban a capturar). En la Figura 3-16 se muestran varios fotogramas del vídeo, donde se ve el cajero falso (aunque con apariencia de ser un cajero normal, con su pantalla en funcionamiento, lector de tarjetas y teclado), el proceso de desmontaje del cajero falso y el cajero auténtico.

Figura 3-16: Cajero falso encima de uno verdadero

Hay otro tipo de equipamiento fraudulento que se instala en comercios, concretamente en los denominados puntos de venta (PoS, *Points of Sales*). En estos casos se aprovecha la obligatoriedad de los clientes de pagar sus artículos para obtener los datos de sus tarjetas. En ocasiones los delincuentes son los propios dueños de las tiendas, o bien empleados deshonestos. También se han conocido casos en los que los dueños no eran cómplices, como ocurrió en una tienda de la cadena Nordstrom en Florida, E.E.U.U. Allí se descubrieron varios dispositivos que capturaban las pulsaciones de teclas (*keyloggers*) conectados a las cajas registradores. Según se pudo comprobar posteriormente por las grabaciones de las cámaras de seguridad, varias personas distrajeron a los empleados de la tienda mientras otra tomaba fotos de los equipos que se utilizaban para cobrar los artículos. Varias horas más tarde se repitió la situación en la que se mantuvo distraídos a los empleados de la tienda, mientras otra persona instalaba rápidamente algo en las cajas registradoras. Lo que se había instalado era un pequeño dispositivo que se intercalaba en la conexión del teclado y del lector de tarjetas, con formato PS/2, interceptando los datos en tránsito. Los delincuentes tuvieron en consideración hasta el color de los conectores, pues el *keylogger* instalado tenía el mismo color que los cables originales del equipamiento de punto de venta(121). Estos dispositivos son bastante sofisticados, ya que pueden enviar los datos interceptados por correo electrónico, conectándose a alguna red WiFi, y disponen incluso de memoria y batería suficiente para estar funcionando durante años. En la Figura 3-17se muestra uno de ellos, a la venta por 139 dólares, que incluye 2 GB de memoria y batería para funcionar durante 7 años. Se vende con una aplicación para Windows que permite al comprador acceder

fácilmente al dispositivo a través de Internet, y soporta 50 disposiciones de teclado para contemplar distintos idiomas. Tiene además versiones USB y PS/2(122).

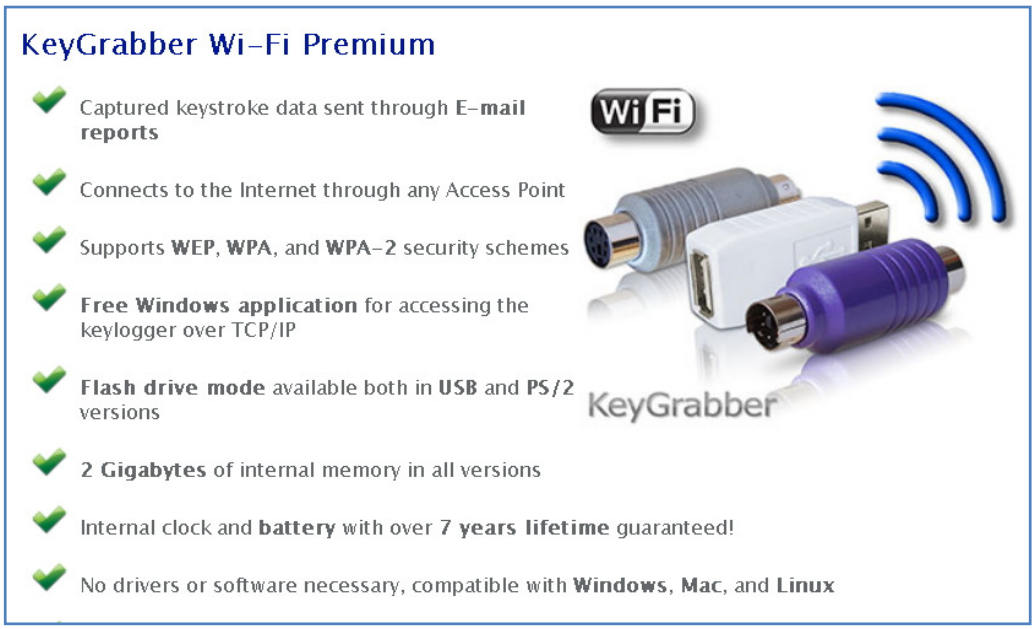


Figura 3-17: Dispositivo de captura de teclado y ratón

Una de las últimas acciones que se han descubierto, explicada en el conocido *Chaos Communication Congress* celebrado en Hamburgo en 2013, consiste en infectar los cajeros electrónicos con *malware*. Mediante una memoria USB se introduce código dañino especialmente diseñado para operar con el cajero en cuestión, de manera que no se observa ningún daño físico ni modificación en el mismo. El cajero opera normalmente, pero cuando se le introduce un código concreto de 12 dígitos, entra en un modo especial de trabajo que permite listar la cantidad de billetes que hay de cada valor, y a continuación extraerlos sin tener que cargarlos a ninguna cuenta ni usar ninguna tarjeta. Es curioso que el supuesto "cerebro" de esta operación no parece fiarse de quien ejecuta la acción en el cajero; de hecho, a la persona presente en el cajero se le muestra en pantalla una serie de números, que debe indicar por teléfono al jefe de la banda; éste le responderá con otro código, que el ladrón introducirá en el teclado del cajero para poder extraer finalmente el dinero. Los ciberdelincuentes que han diseñado este ataque han demostrado un conocimiento muy profundo del modo de operar de los cajeros automáticos, y han programado el código dañino de una manera que es difícil de analizar(123).

En definitiva, puede verse que hay muchas formas de engañar a los usuarios de cajeros y comercios para hacerse con los datos de sus tarjetas de crédito y débito, datos que, como se ha comentado, serán utilizados de varias maneras fraudulentas por los ciberdelincuentes.

3.5.3. PROPAGACIÓN DE CÓDIGO DAÑINO

Como se indicaba anteriormente, hay ciberdelitos que no requieren el uso de *malware*, ya que simplemente utilizan la inocencia o desconocimiento de los usuarios para

robarles cierta información, o bien la instalación de equipos a propósito en cajeros automáticos o comercios para robar datos de tarjetas de crédito o débito. Otros ciberdelitos por el contrario sí requieren el uso de *malware* diverso. En estos otros casos, ¿cómo llega el *malware* a los equipos de las víctimas?

Para empezar, es conveniente hablar sobre las vulnerabilidades de los sistemas. Suele ocurrir que los sistemas operativos, aplicaciones o incluso el propio hardware donde se ejecutan tengan algún tipo de vulnerabilidad. Al software que aprovecha vulnerabilidades para realizar alguna acción indebida se le denomina *exploit*. Por acción indebida se entiende la ejecución de código con privilegios superiores al del usuario que está utilizando la máquina (es lo que se denomina "escalada de privilegios"), de tal manera que se consigue obtener acceso a recursos que normalmente están protegidos; así, es posible la escritura en algún tipo de medio de almacenamiento del sistema local o en red, el acceso a estructuras internas del sistema operativo (como el registro de las distintas versiones de Windows) o incluso la posibilidad de controlar el hardware sin pasar por los filtros de los sistemas operativos. En ocasiones se construyen herramientas completas que engloban distintos *exploits* y que se venden en el mercado negro a los cibercriminales; estas herramientas se denominan *exploit kits*. Es importante distinguir entre el *malware* concreto con que se quiere infectar a una víctima y el *exploit*: como ejemplo, considérese que se quiere comprometer un sistema con un *backdoor*. En ese caso hay dos opciones para conseguirlo: se puede integrar el *backdoor* en otro programa aparentemente inocuo, como una calculadora, de tal manera que si el usuario ejecuta la calculadora, el *backdoor* quedará instalado en su sistema y permitirá acceso remoto a voluntad del atacante. Por otra parte también se puede integrar un *exploit*, es decir, un código que aproveche una vulnerabilidad del sistema, en un programa aparentemente inofensivo como la calculadora. En este caso el *exploit* realiza una función intermedia, pues puede, una vez ejecutada la calculadora, contactar con un servidor externo y descargarse un *backdoor*. El *exploit* puede desaparecer del sistema una vez realizada su función, lo que hace más difícil para los equipos de seguridad detectar posteriormente cuál ha sido la forma de entrada del *malware* para poder implementar alguna solución. El *exploit* a su vez puede añadir más vulnerabilidades al propio sistema infectado, de manera que sea posible comprometerlo con más software maligno adicional. En adelante, se hablará de archivos infectados con *malware* para hacer referencia a ambas posibilidades indistintamente, pues en cualquiera de los casos el resultado es el mismo.

Los archivos en los que se esconde el *malware* suelen ser documentos PDF, archivos de aplicaciones informáticas (como Microsoft Word, Excel o Access), archivos multimedia y otros. Estos archivos aprovecharán vulnerabilidades de las aplicaciones con las que se suelen abrir o del sistema operativo que las soporta. Una vez que el ciberdelincuente prepara estos archivos infectados, solo queda hacerlos llegar a los equipos de las víctimas.

La forma más directa es el envío de código dañino directamente por correo electrónico. Ya se ha hablado del *spam* como técnica de envío masivo de correo no solicitado, y precisamente otro uso del mismo es el de envío de ficheros con *malware*. Afortunadamente los antivirus en los sistemas intermedios y finales suelen actuar y

bloquear bastante este software indeseado, y tanto los servidores de correo corporativos como los propios proveedores de servicios de correo electrónico ofrecen servicios de bloqueo de *malware* que logra interceptar un porcentaje muy elevado del mismo. Aun así se sigue utilizando la técnica de envío directo de software maligno por correo electrónico, simulando en muchos casos contener información útil para el receptor (informes de mercado, documentación de nuevos productos, etc.).

3.5.4. ATAQUES BASADOS EN WEB

Pero el envío directo de *malware* no es la única forma de infección. Últimamente se ha visto un incremento notable en otra técnica llamada **ataque basado en web**. El procedimiento es sencillo: el usuario víctima visita una página web y, sin ser consciente, su equipo es contagiado. Para ello los ciberdelincuentes podrían instalar, configurar y publicar un servicio web que contenga *exploits* para aprovechar vulnerabilidades de los sistemas visitantes. Esto requiere obligar de alguna manera a las víctimas a que visiten estos sitios web, algo que no es fácil a priori. En lugar de eso, lo que se suele hacer es comprometer algún sitio web lícito, insertando directamente en él el *malware* que se quiera propagar o bien incorporando en la web lícita enlaces al servidor preparado previamente por los cibercriminales y que almacena el *malware*(124). En muchos casos estos enlaces en la web lícita no van directos al servidor del *malware*, sino que se producen varias redirecciones intermedias hasta llegar al que contiene el código dañino, de manera que se hace más difícil el seguimiento. Ahora bien, ¿cómo consiguen los ciberdelincuentes comprometer el sitio web lícito? Hay varias formas: se puede aprovechar alguna vulnerabilidad del software de gestión de contenidos del servidor web, puede atacarse la infraestructura que hay dentro de la red interna del servidor web (bases de datos, software de control interno), o incluso se pueden usar técnicas de *phishing* o *spyware* dirigidas a los administradores web para obtener sus claves de acceso a los sistemas. Otra variante utilizada para comprometer sitios web lícitos es el llamado ***malvertising***[48], que consiste en contratar legalmente anuncios en páginas web, e inyectar a continuación algún código dañino en los anuncios que consigan llevar el *malware* a los visitantes. En este caso no se requiere que los usuarios sigan ningún enlace como ocurre al recibir *spam*, sino que basta con que el anuncio se muestre en el navegador para que se pueda producir la infección. Esta técnica se utilizó en el popular sitio myspace.com hace algunos años, donde un cartel publicitario logró infectar a millones de usuarios con un troyano aprovechando una vulnerabilidad del navegador de Windows *Internet Explorer* al trabajar con archivos de imágenes en formato WMF (*Windows MetaFile*)(125). El periódico *The New York Times* también sirvió de plataforma para otro tipo de *malvertising* que intentaba convencer a los usuarios para que instalaran un antivirus falso(126)(127). De acuerdo con el informe de la referencia (78) de la empresa Symantec, durante el año 2012 el número de ataques basados en web se incrementó en un tercio, y desde 2010 a 2012 se multiplicó por 20; el mismo informe indica que en una prueba con un software propio de escaneo, la mitad de los sitios

[48] *Malvertising* viene de las palabras en inglés *malware* y *advertising*, o bien de *malicious advertising*, publicidad maliciosa.

probados estaba infectado por *malvertising*. Teniendo en cuenta que no dejan de aparecer vulnerabilidades tanto en los navegadores y sus complementos como en los distintos servidores web, es de esperar que este tipo de ataques siga aumentando en el futuro. Para ilustrar la importancia de los ataques basados en web, se indican a continuación algunos datos extraídos del citado informe de Symantec referidos a 2012:

- el número de dominios web con código dañino era de 74.000;
- el 23% del correo enviado con *malware* incorporaba enlaces a direcciones de sitios web con contenido dañino;
- el 61% de sitios web con código dañino son sitios legítimos que han sido comprometidos e infectados;
- 1 de cada 532 sitios web estaba infectado por *malware*;
- el 53% de los sitios web analizados tenían vulnerabilidades aprovechables;
- la mitad de los sitios web analizados en el estudio estaban infectados con *malvertising*.

Hay otras variantes para conseguir hacer llegar el código dañino a las víctimas. Como ejemplo, se ha observado en alguna ocasión que ciertos ciberdelincuentes venden vehículos en Internet pero no facilitan fotos en la web de venta. Para poder tenerlas, los posibles compradores las tienen que pedir, y se les envían las fotos como adjuntos a correos electrónicos, o bien la víctima recibe un enlace a alguna galería de fotos en Internet. En ambos casos, las fotos contienen *malware* y se redirige al usuario a sitios web que son idénticos a los portales de venta donde vieron el anuncio original, aunque estos nuevos sitios web están bajo el control de los ciberdelincuentes. Suelen dar incluso soporte técnico y telefónico en esta nueva web, y llegan a recomendar algún servicio *escrow* que, por supuesto, también pertenece a los ciberdelincuentes(128).

3.5.5. ATAQUES DIRIGIDOS

Hasta ahora se han comentado tipos de código dañino y técnicas utilizadas por los cibercriminales para, usando dicho código, cometer algunos de sus delitos. Los procedimientos seguidos suelen ir encaminados a obtener provecho de cualquier usuario o sistema que pueda ser vulnerable, sin distinguir en algunos casos qué tipo de usuario será el que se convierta en víctima. Sin embargo, en los últimos años se ha visto una tendencia interesante y a la vez alarmante: los distintos ataques no se lanzan de manera general e indiscriminada hasta que alguien caiga en la trampa, sino que tienen como objetivo a alguna persona concreta, equipo o grupo de trabajo de alguna empresa o institución. A estos ataques se les denomina **ataques dirigidos**.

Si se aplica el concepto de ataque dirigido a las campañas de *phishing*, se observa que en muchos casos los ciberdelincuentes envían correos electrónicos a determinados destinatarios y con ciertas características especiales. Así, por ejemplo, es habitual que se lancen campañas de *spam* a usuarios de una determinada entidad bancaria o a clientes de algún establecimiento comercial concreto. Las comunicaciones electrónicas recibidas por las víctimas potenciales suelen estar personalizadas hasta cierto punto, de tal manera que se saluda al usuario por su nombre de pila, o bien se le hace referencia a alguna compra realizada recientemente; en otros casos se le hace creer que el correo

electrónico procede de alguna empresa con la que ha tenido trato tiempo atrás, o que está relacionada con alguna gestión reciente realizada en su entorno profesional o familiar. La información no es demasiado difícil de conseguir para los cibercriminales, pues la proliferación de las redes sociales y la poca precaución de sus usuarios para mostrar públicamente datos sobre sus actividades o sus gustos suele bastar para recabar datos clave. En otros casos se utiliza algún tipo de spy*ware* para conseguir algo más de información del usuario. Estas técnicas consiguen bajar la guardia de las víctimas, que ven cierta legitimidad en los correos recibidos y pueden caer más fácilmente en la trampa. A este tipo de ataque dirigido se le denomina ***spear phishing***[49].

Por otra parte, también existen los ataques dirigidos basados en web. Esto responde a una forma mucho más elaborada de trabajar para conseguir un determinado objetivo. Para usar esta técnica, los cibercriminales eligen en primer lugar alguna víctima de la cual puedan sacar algún tipo de provecho. Estudian sus costumbres de navegación en la web, viendo el tipo de sitios que habitualmente visitan (posiblemente accediendo a las *cookies* almacenadas en su navegador habitual o bien, una vez más, gracias a las redes sociales). A continuación analizan los propios sitios web más visitados por la víctima, buscando vulnerabilidades en los servidores, en las bases de datos o en las implementaciones de las páginas. Una vez encontradas, inyectan algún tipo de código malicioso en el servidor web, con objeto de redirigir a la víctima a otro servidor comprometido, que estará esperando con alguna vulnerabilidad, posiblemente de día cero[50], para infectar al usuario y posteriormente conseguir el objetivo deseado. De esta manera, no se busca o ataca al usuario directamente, como ocurre con el *spear phishing*, sino que se le espera tranquilamente a que caiga en la trampa, sabiendo por el estudio previo realizado que en algún momento pasará por el sitio web comprometido. Esta técnica recuerda a la que utilizan algunos depredadores en zonas semidesérticas o de sabana, donde, en lugar de perseguir a sus víctimas para atraparlas, esperan junto a algunos charcos o abrevaderos a que éstas se acerquen a beber. Por ese motivo, en el mundo de las nuevas tecnologías este ataque recibe el nombre de ***watering hole***, expresión en inglés que se refiere a las mencionadas acumulaciones de agua.

El procedimiento recién descrito es la forma general de conseguir el objetivo del ciberdelincuente, aunque suele complementarse con otras técnicas de ingeniería social, con ataque previos de tipo *spear phishing* o incluso algún *malware* diseñado expresamente para atacar a la víctima o extraerle previamente algún tipo de información en alguna fase del ataque (como se ha indicado en el caso del robo de *cookies* del navegador). En los ataques dirigidos se observa que los procedimientos criminales implican un detallado y meticuloso estudio previo de la situación, mostrando

[49] El término está bien elegido: *spear* significa en inglés arpón, y el término *phishing* tiene relación directa con *fishing*, o sea, pesca, de manera que la expresión significaría "pesca con arpón".

[50] Se denomina vulnerabilidad de día cero a aquella que aún no es conocida públicamente, y ni siquiera el fabricante del software la conoce, de tal manera que los cibercriminales pueden aprovecharla sin temor a que ningún producto antivirus detecte los *exploits* utilizados.

una premeditación y un grado de preparación superiores a los habituales en otro tipo de delitos. Con estos antecedentes se puede entender que el porcentaje de éxito en este tipo de ataques sea alto. No es raro por otra parte que los principales casos de ataques dirigidos tengan que ver con el ciberespionaje, tanto en el entorno industrial como en el gubernamental.

Existe otra variante a los ataques dirigidos; en ocasiones no es fácil llegar al objetivo último por parte de los cibercriminales, debido a medidas de seguridad elevadas en las pretendidas víctimas o a un alto grado de concienciación en la seguridad en ese entorno. En estos casos, los delincuentes utilizan los llamados **ataques indirectos**: estudian las relaciones externas de la empresa o institución que se quiere atacar, y eligen como nuevas víctimas a los proveedores o a intermediarios en las cadenas de suministro, logísticas o de flujo de trabajo. En muchos casos estos proveedores o intermediarios son empresas más pequeñas, con menor presupuesto y con bastantes menos recursos y medidas de seguridad en sus sistemas informáticos. Esto las hace más vulnerables, y más fáciles de atacar para los cibercriminales. Una vez los sistemas de estas empresas más pequeñas están comprometidos, es mucho más fácil llegar a la empresa o institución que se pretendía atacar inicialmente, por medio de interconexiones de red corporativas de confianza, utilizando el sistema de correo electrónico de la empresa pequeña para lanzar más ataques de *spear phishing* al objetivo real, etc.

También se ha visto cómo en algunas ocasiones los ataques no se dirigen directamente a la cúpula de las empresas objetivo, sino que se centran en departamentos accesorios (I+D, marketing…). Éstos son casos similares a los de los ataques indirectos, pues la parte alta de la jerarquía empresarial y oficial suele estar más protegida, y es más fácil vulnerar la seguridad de departamentos accesorios que sirven de trampolín para llegar posteriormente al objetivo final.

3.5.6. REDES ZOMBI Y KITS DE HERRAMIENTAS

Es necesario completar el panorama de técnicas de infección y ataque usadas por los cibercriminales con algunos conceptos que suelen aparecer en noticias relacionadas con el cibercrimen muy frecuentemente. Debe considerarse primeramente que en ocasiones el *malware* mencionado en este capítulo se instala de manera individual en multitud de equipos de usuarios, ya sean particulares, empresariales o institucionales. El daño que pueden hacer depende de la finalidad para la que han sido diseñados en cada caso (*spyware*, *keylogger*, etc.) y afectará al sistema infectado y al usuario que lo utilice. Sin embargo, es habitual que cierto tipo de *malware* se propague por miles o millones de equipos en todo el mundo, y formen una red organizada para generar daño, realizar alguna acción o sacar algún tipo de provecho. Los sistemas infectados, componentes de esta gran red, realizarán acciones diferentes según lo que se le ordene en cada momento desde un centro denominado de “mando y control” (C&C, del inglés *Command and Control*), aunque siempre sin el conocimiento del usuario de los sistemas.

Estas redes de equipos infectados por algún *malware* con diversos objetivos y con posibilidad de ser controladas remotamente se conocen como **redes zombi** o ***botnets***[51].

Los usos de las redes zombi son muy variados: pueden utilizarse para enviar correos masivos (*spam*), sea cual sea la intención de dichos correos (buscar víctimas de *phishing*, propagar *malware*, enviar direcciones de servidores web comprometidos, etc.), o también para realizar ataques de denegación de servicio distribuido, como se avanzó en la página 62. En cualquiera de los casos constituyen una herramienta muy potente para los cibercriminales, dado que permiten realizar las acciones indicadas casi con garantía de total anonimato para quien las está dirigiendo.

Los equipos que pertenecen a las redes zombi (los propios zombis) están siempre infectados con algún tipo de *malware*. Lo habitual es que sean del tipo *backdoor*, aunque no se puede categorizar de una única manera el software maligno presente en los zombis, pues suelen realizar muchas acciones. Como ejemplo, considérese el famoso *malware* Zeus; estaba diseñado originalmente para robar información de tipo bancario, y lo consigue realizando distintas acciones: roba información de los equipos infectados, mediante técnica de *keylogging*; captura la pantalla; lanza ataques DDoS; intercepta las conexiones realizadas mediante los protocolos FTP y POP3[52], así como las peticiones HTTP y HTTPS; lleva a cabo ataques de *phishing*; etc. Algunos troyanos incluso tienen la posibilidad de cargar módulos de *malware* adicionales y de actualizar manual o automáticamente partes del troyano. La manera de infectar a un equipo con el *malware* correspondiente para convertirlo en un zombi es cualquiera de las que se han visto anteriormente, aunque en estos casos también se ha detectado una gran cantidad de propagación mediante las redes de intercambio de igual a igual o P2P. Es habitual que se utilicen también para la infección troyanos que simulan (y de hecho son) generadores de números de serie para software comercial, o software que realiza algún tipo de modificación en el sistema (*patch*) para permitir la ejecución ilegal de este software comercial.

Las redes zombi suelen tener una infraestructura de mando y control. Normalmente habrá un equipo (denominado "*botmaster*") que enviará instrucciones a los sistemas infectados para que realicen determinadas acciones, y recibirá información de estos sistemas comprometidos. Es necesario, por tanto, un canal de comunicación entre el *botmaster* y los equipos que conforman la red; para ello pueden utilizarse estructuras centralizadas, en las que un servidor se comunica con los zombis directamente (habitualmente mediante servidores *Internet Relay Chat*[53] o IRC[54], usando redes sociales

[51] Término que viene de las palabras inglesas *robot* y *network*, y que por tanto da idea de una red de robots.

[52] *Post Office Protocol* 3, protocolo utilizado para recoger correo electrónico de un servidor por parte de un cliente.

[53] IRC hace referencia a sistemas de comunicación en tiempo real mediante mensajes de texto; se basa en servidores que albergan "salas" o "canales" y clientes que se conectan a distintas salas para chatear entre sí.

como *Twitter*, por medio de blogs, mediante comunicación HTTP o incluso a través del software *Skype*), o bien pueden usarse estructuras distribuidas de tipo P2P[55] (como hace la red *ZeroAccess*, también conocida como *ZAccess* o *Sirefef*). Esta última posibilidad hace mucho más difícil la tarea de seguimiento e investigación de las redes zombi, a la par que consigue una infraestructura de comunicación más robusta para la misma. En todos los casos estas comunicaciones se llevan a cabo de manera opaca para el cibercriminal que controle estas redes, que suele limitarse a acceder a un sistema de gestión web (llamado genéricamente el "panel de control"), cómodo y visualmente atractivo, que le permite dar órdenes, lanzar ataques, recabar información robada, mostrar estadísticas de equipos infectados agrupados por países, por sistemas operativos, etc. todo ello de forma fácil y clara. En la Figura 3-16se muestra un ejemplo del panel de mando y control de Zeus; en concreto, puede verse un formulario de búsqueda, a través del cual se pueden localizar resultados de datos robados (credenciales FTP, tráfico HTTP y HTTPS, y otros).

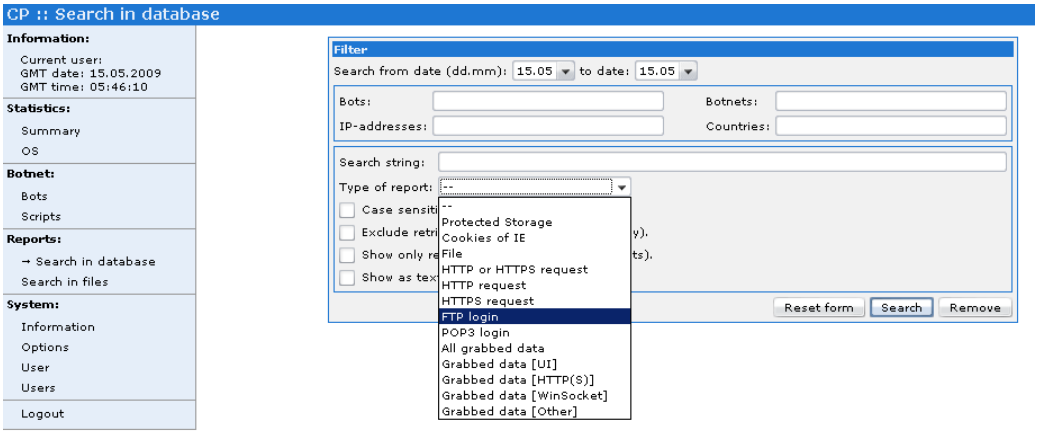


Figura 3-18: Panel de mando y control de Zeus

En la Figura 3-19 se puede ver un ejemplo de captura de contraseña al acceder un sistema infectado a un sitio web.

[54] Para ver un mapa actualizado cada hora que muestra la actividad de algunos servidores de mando y control de redes zombi, puede visitarse la dirección http://www.team-cymru.org/Monitoring/Malevolence/irccnc.html

[55] Las redes zombi que usan P2P para su estructura de mando y control son más difíciles de detectar y eliminar; véase informe en http://www.ieee-security.org/TC/SP2013/papers/4977a097.pdf

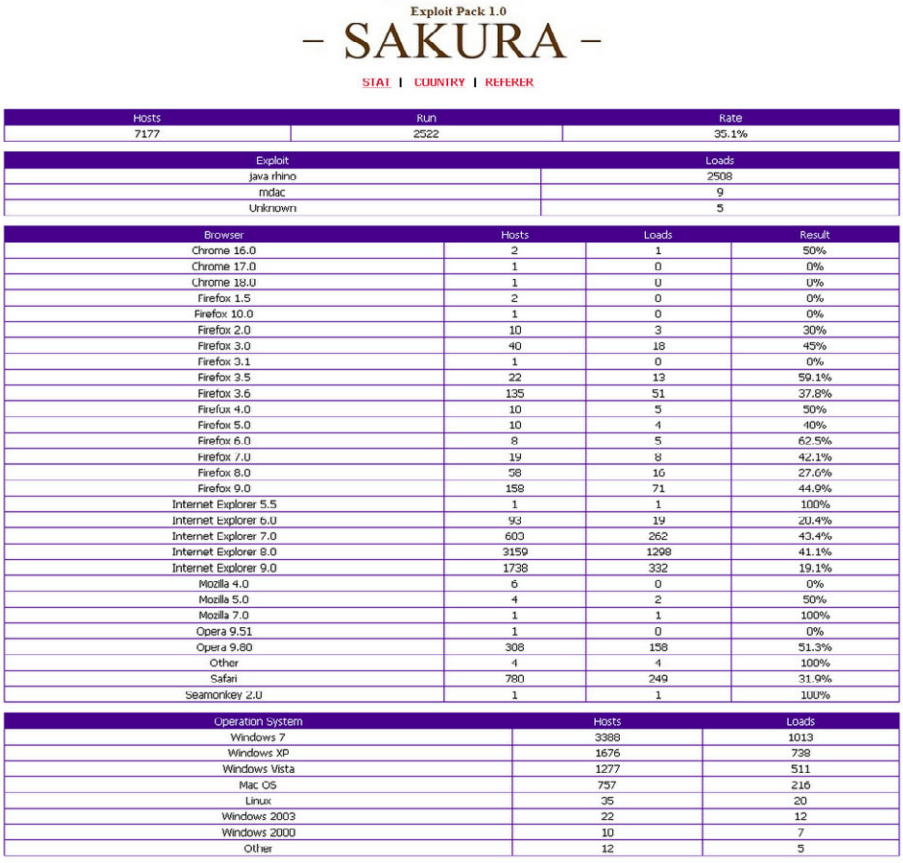
View report (HTTP request, 172 bytes)	
Bot ID:	**bot_10000001**
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	30.09.2009 14:16:03
GMT:	-8:00
Session time:	04:35:50
Report time:	30.09.2009 21:15:41
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	http://www. bank.com/login.php

```
http://www. bank.com/login.php
Referer: http://www. bank.com/login.html
Keys: admintestswordfish1234567890
Data:

username=admintest
password=swordfish
pinnumber=1234567890
```

Figura 3-19: Ejemplo de captura de contraseña

Las herramientas completas, que incluyen los distintos virus, troyanos, gusanos, etc. y el software encargado de gestionar las comunicaciones de mando y control, interfaz de usuario, actualizaciones, etc. se agrupan en lo que se conocen como **kits de herramientas** o ***toolkits***. Continuando con el ejemplo anterior, Zeus se ha convertido en un kit de herramientas, contando con un completo entorno de distribución, gestión, control y explotación de los equipos infectados. En 2011 el código fuente de Zeus fue filtrado y publicado(129); esto provocó que se diseñaran nuevos troyanos y herramientas basadas en él. Algunos son variantes de la familia de Zeus, como la conocida por GameOver (al ser una banda de criminales con este nombre la que le encargó al autor original de Zeus su modificación a medida). Esta variante fue programada por el propio autor original de Zeus e incluía bastantes mejoras. Otros productos derivados fueron SpyEye y Ice IX(130). En fechas recientes (año 2013) se ha podido comprobar que se encuentra a la venta el código fuente de una variante de Zeus que se auto-replica mediante la red social Facebook y el correo electrónico. El código fuente cuesta entre 160 y 180 dólares de E.E.U.U.; si se quiere adquirir una versión compilada el coste baja al entorno de los 80 a 100 dólares(131). Otros kits muy conocidos son Blackhole, Magnitude, Incognito, Phoenix, Redkit, Sakura, LizaMoon y Nuclear, por citar algunos. En la Figura 3-20 puede verse una parte del panel de control de Sakura, donde se observa el número de equipos infectados y el tipo de *exploit* utilizado, así como los navegadores y sistemas operativos de las víctimas. Es habitual que a las redes zombi formadas a partir de un determinado *malware* o kit de herramientas se les denomine con el mismo nombre que la herramienta. Así, es frecuente encontrar noticias referidas a la *botnet* Zeus (también llamada *Zbot*), o a las *botnets* Cutwail, Kelihos, Maazben, Festi, Nitol, Grum, Sefnit, o Slenfbot, por mencionar solo algunas. En la práctica se utiliza muchas veces el mismo nombre para hablar indistintamente del troyano, del kit de herramientas y de la red zombi formada.



Exploit Pack 1.0

– SAKURA –

STAT | COUNTRY | REFERER

Hosts	Run	Rate
7177	2522	35.1%

Exploit	Loads
java rhino	2508
mdac	9
Unknown	5

Browser	Hosts	Loads	Result
Chrome 16.0	2	1	50%
Chrome 17.0	1	0	0%
Chrome 18.0	1	0	0%
Firefox 1.5	2	0	0%
Firefox 10.0	1	0	0%
Firefox 2.0	10	3	30%
Firefox 3.0	40	18	45%
Firefox 3.1	1	0	0%
Firefox 3.5	22	13	59.1%
Firefox 3.6	135	51	37.8%
Firefox 4.0	10	5	50%
Firefox 5.0	10	4	40%
Firefox 6.0	8	5	62.5%
Firefox 7.0	19	8	42.1%
Firefox 8.0	58	16	27.6%
Firefox 9.0	158	71	44.9%
Internet Explorer 5.5	1	1	100%
Internet Explorer 6.0	93	19	20.4%
Internet Explorer 7.0	603	262	43.4%
Internet Explorer 8.0	3159	1298	41.1%
Internet Explorer 9.0	1738	332	19.1%
Mozilla 4.0	6	0	0%
Mozilla 5.0	4	2	50%
Mozilla 7.0	1	1	100%
Opera 9.51	1	0	0%
Opera 9.80	308	158	51.3%
Other	4	4	100%
Safari	780	249	31.9%
Seamonkey 2.0	1	1	100%

Operation System	Hosts	Loads
Windows 7	3388	1013
Windows XP	1676	738
Windows Vista	1277	511
Mac OS	757	216
Linux	35	20
Windows 2003	22	12
Windows 2000	10	7
Other	12	5

Figura 3-20: Panel de control de Sakura

Al final, las distintas herramientas se combinan para conseguir los objetivos de los ciberdelincuentes. No es raro comprobar que alguna de las redes zombi conocidas se utilizan para propagar algún troyano famoso, pero también es interesante observar cómo ciertos acontecimientos influyen tanto en el uso de las herramientas como en los "negocios" a los que se dedican ciertas bandas de delincuentes. Un ejemplo de ello ocurrió recientemente, en otoño de 2013. Un grupo delictivo utilizaba Cutwail, considerada la mayor red zombi del mundo, muy eficiente en cuanto a la posibilidad de envío de *spam* y ampliamente usada para desplegar una variedad de Zeus llamada Gameover(132), clasificada como troyano bancario. Para la infección se usaba a su vez el Blackhole Exploit Kit. De manera inesperada, el autor del Blackhole Exploit Kit (BHEK), apodado "Paunch", fue arrestado en octubre de 2013. Algunos indicadores de determinadas empresas de seguridad confirmaron que desde el día del arresto (5 de octubre), las campañas de *spam* que se habían identificado que usaban ese *exploitkit* dejaron de estar operativas(133). Esto puede considerarse lógico y normal, pero esa no fue la única consecuencia: dado que en los ambientes delictivos se temía que a raíz del arresto podrían descubrirse quiénes usaban el kit BHEK y, por tanto, eran "clientes" de Paunch, un importante grupo cibercriminal dejó de usar dicho kit y pasó a usar otro, conocido como Magnitude (anteriormente llamado Popads)(134)(135)(136). Este otro

kit propaga un *malware* distinto, llamado ZeroAccess, especializado en fraudes de clic, *spam* y minería de Bitcoin[56]. Así, la banda en cuestión pasó de utilizar el troyano bancario Gameover Zeus a usar ZeroAccess, que sirve para cometer otro tipo de delitos. Por tanto, un acontecimiento como la detención de uno de los gestores de herramientas de explotación ha hecho cambiar las actividades y el modelo de negocio de una banda de delincuentes.

Al igual que se comentó anteriormente sobre la tendencia de los ciberdelincuentes dedicados al *phishing* a través de *spam* de expandir sus actividades a los dispositivos móviles, las redes zombi también están sufriendo el mismo proceso; ya se ha detectado código dañino que afecta a terminales móviles y los integran en *botnets*, quedando el dispositivo a merced del cibercriminal, que puede usarlo para su propio beneficio. Un ejemplo de ello es el troyano y *backdoor* denominado Android.Bmaster, que tras infectar a los móviles con sistema operativo Android, ofrece al atacante beneficios mediante el envío de SMS de tarificación especial y suscripción a servicios de video bajo demanda, aunque también le permite disponer de una amplia variedad de información del dispositivo (IMEI, celda de telefonía móvil donde se encuentra, operador que usa, IMSI[57]), además de poder recibir comandos remotos para realizar llamadas, enviar SMS, enviar el registro de llamadas realizadas, bloquear mensajes de texto entrantes, actualizar la dirección del servidor de mando y control y descargar más código dañino(137)(138).

La incursión de los ciberdelincuentes en nuevos entornos que les sirvan como plataformas de ataques no se queda en los dispositivos móviles. Recientemente se maneja la expresión “Internet de las cosas” (*Internet of Things*, *IoT*) para referirse al conjunto de equipos electrónicos que están conectados a Internet sin ser ordenadores, servidores o dispositivos móviles, e incluyendo *routers* domésticos, consolas de juegos y reproductores multimedia, entre otros. Un informe reciente de una empresa especializada en seguridad denominada *Proofpoint*(139) ha desvelado que entre el 23 de diciembre de 2013 y el 6 de enero de 2014 se produjo una avalancha de envío de correo no deseado que escondía algún tipo de ataque. Lo interesante del estudio es que un 25% de los correos (del orden de 750.000) procedían de más de 100.000 equipos domésticos como los comentados, incluso algunos enviados por televisores y algún frigorífico conectado a Internet(140)(141)(142). Esto demuestra que el mundo del cibercrimen está ampliando sus ámbitos de actuación más allá de lo que podría imaginarse hace unos años.

[56] Se tratará el tema de Bitcoin y la criptomoneda en el punto 3.6.

[57] *International Mobile Subscriber Identity*, identidad internacional de abonado móvil: es un número que identifica a cada usuario de telefonía móvil, incorporando un código de país y un código de operador, además de un número del propio abonado. Es distinto del número de teléfono.

3.5.7. APT

El mundo del *crimeware* ha ido evolucionando de acuerdo con las nuevas posibilidades ofrecidas y con la imaginación de los distintos actores implicados. Se ha llegado a técnicas de sofisticación inimaginables hace varios años. Una de ellas, muy sofisticada, de las más peligrosas y efectivas, a la vez que extendidas, es la llamada **APT** o *Advanced Persistent Threat* (amenaza persistente avanzada). Corresponde este acrónimo a una operación en la que interviene distinto tipo de software que se infiltra en una red objetivo con el propósito de robar información de manera masiva y constante y además permanecer oculto durante el mayor tiempo posible. Se ha utilizado (y se sigue utilizando) principalmente en campañas de ciberespionaje con objetivos políticos, militares y económicos principalmente, y responde a un tipo de ataque muy dirigido. A primera vista puede parecer que sigue un esquema de funcionamiento similar al de las *botnets*, aunque realmente es mucho más complejo. Como dice el Dr. Eric Cole en su libro "*Advanced Persistent Threat. Understanding the danger and how to protect your organization*", "*Los APT no son una botnet. No es malware. Es el ADN de un grupo adversario*"(143).

Cuando se lleva a cabo un ataque APT el primer paso, tras elegir el objetivo, es infiltrar algún tipo de *malware* en la red de la organización, institución o empresa víctima. Este conjunto de software realizará en primer lugar un estudio de los distintos equipos existentes en la red (no solo ordenadores, sino todo tipo de dispositivos que eventualmente podrían ser vulnerables, como impresoras, servidores de impresión, servidores de disco, escáneres, etc.), así como de la topología de la misma. A continuación realiza el acceso a los sistemas vulnerables, infectándolos de la manera más adecuada. Tras ello estudia qué tipo de información almacena (ficheros, tráfico en tránsito con la red local o con redes externas, etc.). Posteriormente realizará el robo de los datos, filtrándolos al exterior de manera discreta para no levantar sospechas en los distintos dispositivos de vigilancia que la organización pueda tener. En paralelo va realizando labores de infección en más sistemas vulnerables, pero siempre manteniendo unas pautas de actuación en las que prima la necesidad de no ser detectado en ningún momento, con objeto de mantener la presencia durante largos períodos de tiempo. No es habitual que se conozcan públicamente los casos de intrusión descubiertos, dada la naturaleza de las organizaciones implicadas (tanto las víctimas como las que realizan los ataques), aunque sí han salido a la luz algunos; tal es el caso de la empresa japonesa *Mitsubishi Heavy Industries*, donde se encontraron unos 80 equipos infectados con 8 tipos distintos de *malware*(144). Esta empresa se dedica a la fabricación de componentes militares para submarinos, misiles y equipamiento nuclear. También fue víctima de este tipo de ataques la Oficina de Su Santidad el Dalai Lama (OHHDL, *Office of His Holiness the Dalai Lama*), el gobierno tibetano en el Tíbet y algunas organizaciones afines, entre los años 2007 y 2009. Muchos de sus ordenadores estaban infectados con *malware*. Tras la sospecha de la oficina del Dalai Lama, se investigó el caso, encontrándose una red enorme de ciberespionaje de ámbito mundial bautizada como "*Ghostnet*". Esta red tenía comprometidos alrededor de 1300 ordenadores en más de 100 países, afectando no solo a organizaciones relacionadas con el Dalai Lama, sino también a muchas embajadas y ministerios de asuntos exteriores. Los servidores desde

los cuales se enviaban órdenes a la red APT y que recibían la información filtrada estaban localizados en China(145)(146).

3.6 WEB PROFUNDA Y CRIPTOMONEDA

La mayor red de datos pública y abierta, Internet, ofrece la posibilidad de acceder a millones de servidores, fuentes de información, plataformas de juegos, servicios de mensajería instantánea y de comunicaciones variadas, portales de comercio electrónico y de compraventa de artículos, foros, blogs, sitios oficiales en los que poder hacer trámites y un sinfín más de posibilidades. Es relativamente fácil llegar al servicio que se quiere utilizar: habitualmente los usuarios navegan por direcciones que le han sido facilitadas directamente por algún medio (publicidad, información en medios de comunicación, redes sociales, comentarios de otros usuarios, enlaces en otras páginas web, etc.), aunque lo habitual cuando se quiere encontrar algún servicio al cual no se ha accedido anteriormente es acudir a alguno de los grandes buscadores generales existentes. De esta forma es posible encontrar prácticamente lo que uno desee. Sin embargo, no todo el contenido accesible está indexado por los buscadores; hay una gran cantidad de información que, aunque pueda estar disponible si se intenta llegar a ella, no aparece en los resultados de ningún servicio de búsqueda. Se estima que solo un 5% de la información disponible está catalogada en los buscadores; el resto no aparece cuando cualquier usuario realiza alguna consulta al respecto. Esto indica que existe una enorme cantidad de información almacenada y de hecho es difícil llegar a hacerse una idea de todo lo que puede conseguirse en esta red. De forma general, a toda la información que no está accesible directamente ni catalogada en las bases de datos de los buscadores se le denomina **web profunda**, **invisible** u **oculta**, o ***deep web***.

Los motivos por los que no toda la información está disponible en los buscadores son varios. Hay sitios web que no permiten que los robots de los buscadores accedan a sus páginas; asimismo hay multitud de páginas a las que no se puede acceder directamente si no es con algún tipo de credencial, y también hay servidores que exigen algún tipo de consulta para poder llegar a todas las páginas (piénsese en diccionarios online, por ejemplo). En algunos casos hay información almacenada y accesible, pero está cifrada para que solo ciertos usuarios puedan interpretarla, por lo que su contenido no puede ser catalogado. También debe tenerse en cuenta una enorme cantidad de tráfico e información de redes de intercambio P2P (BitTorrent, Donkey y otras). Estas redes operan de tal manera que no es posible establecer un catálogo centralizado y único de información, constituyendo una parte importante de la web oculta.

Por otra parte, con el transcurrir del tiempo desde que se iniciara la interconexión de redes y sistemas para formar lo que actualmente conocemos como Internet, algunas de las preocupaciones de los usuarios han sido la confidencialidad, el anonimato y la posible censura en el acceso a los contenidos. En ocasiones ha sido necesario transferir información a conocidos, empleados o colaboradores de cualquier ámbito de tal manera que las comunicaciones no fueran accesibles para cualquiera que pudiera interceptarlas en tránsito. Esa necesidad de transferencia privada evolucionó posteriormente hacia la

conveniencia de disponer de servicios de consulta de documentos también privados, siendo necesario inventar algún tipo de sistema que permitiera ocultar la propia existencia de esos documentos. Por otra parte el anonimato ha sido buscado frecuentemente para no permitir que se pudiera seguir el rastro de las actividades de los usuarios en Internet, ya que esa información se puede considerar privada y puede ser usada eventualmente con fines maliciosos por parte de quien pueda conseguirla (entidades comerciales, servicios gubernamentales o incluso grupos cibercriminales, por ejemplo). En cuanto a la censura, es conocido que los gobiernos de ciertos países establecen férreos controles sobre la información a la cual tienen acceso sus ciudadanos, habitualmente por motivos políticos. Para cumplir con estas funciones de anonimato y confidencialidad y poder saltar la censura de ciertos gobiernos se han ido creando redes aprovechando la infraestructura existente, redes que se pueden considerar como superpuestas a Internet y en las que se han conseguido, al menos en parte, estos objetivos. Estas redes exigen habitualmente el uso de un software específico, que cumple con los requisitos de comunicación especificados de antemano para conseguir el anonimato y el acceso a ciertos servicios. Cada una de estas redes se considera, a su vez, una red oculta, dentro de la web oculta general que existe en todo Internet.

Son varias las redes ocultas implementadas. Así, por ejemplo, en el año 2000 surgió Freenet, con el objetivo de vencer la censura y proporcionar anonimato en las comunicaciones. Esta red se basa en tecnología P2P, y sigue una filosofía de estructura distribuida que opta por almacenar trozos de información en los equipos de los usuarios que participan en la red. Cuando se necesita recuperar algún documento, se deben encontrar los trozos sueltos guardados en diversos equipos; cada ordenador que forma parte de la red realiza varias funciones, pues almacena algunos segmentos, retransmite las peticiones de ficheros y también los trozos de documentos que se hayan solicitado, aunque sin saber exactamente quién pide qué fichero, ni tampoco teniendo acceso al documento completo. Además las transferencias se realizan de manera cifrada. Hay básicamente dos modos de trabajo: se puede intercambiar información con cualquier otro nodo conectado a Freenet, o bien se puede trabajar en modo de alta seguridad solo con aquellos que se hayan añadido anteriormente como nodos de confianza(147). En la práctica, para trabajar en Freenet solo hay que descargar e instalar un software existente para las plataformas más usadas (Linux, Mac OS X, Windows).

También se conoce la red oculta I2P, *Invisible Internet Project* (Proyecto de Internet Invisible), nacida en 2002 con el objetivo de establecer una capa de red alternativa que permitiera el establecimiento de servicios de uso habitual de forma anónima y segura(148). Se basa también en comunicaciones cifradas y distribución P2P de información. Dispone de aplicaciones propias para servicios de alojamiento web, intercambio de archivos, almacenamiento distribuido de información, correo electrónico y mensajería instantánea, entre otros. Para acceder a los servicios hay que descargar e instalar, como es habitual en este tipo de redes, un software específico (denominado genéricamente "*router* I2P" y escrito en Java), que convierte a los equipos de la red en nodos de la misma. En su funcionamiento habitual se establecen túneles entrantes y salientes por los que circula la información sometida a cuatro capas de cifrado, y los

extremos de las comunicaciones se identifican mediante sus claves públicas, de tal manera que ningún nodo puede conocer el remitente o el destinatario reales de las comunicaciones.

Quizá una de las redes ocultas más conocidas y usadas actualmente es la denominada TOR(149), nombre que viene de *The Onion Router*, literalmente "el *router* cebolla", expresión que a su vez procede de la forma de comunicación que implementa esta red. Sus orígenes tienen que ver con el proyecto "Onion Routing"(150), relacionado con el Laboratorio de Investigación Naval de la Marina de E.E.U.U. (U.S. Naval Research Laboratory(151)). TOR corresponde a la segunda y tercera generaciones del proyecto, y tiene también como objetivo principal el anonimato en Internet; para conseguirlo, establece una estructura de nodos que ejecutan el software correspondiente, y que pueden realizar funciones de cliente y, opcionalmente, de retransmisores. Cuando un cliente quiere realizar algún tráfico de manera anónima, elige 3 nodos de la red para que se establezca un circuito o túnel virtual, y a partir de entonces toda la información se cifra 3 veces consecutivamente, uno para cada nodo. Cuando le llega la información desde el cliente al primer nodo, éste descifra lo recibido (que se cifró con la clave pública de este primer nodo), comprueba cuál es el siguiente nodo del túnel y le envía la información. El segundo nodo la recibe, realiza la misma operación de descifrado con su clave privada, y retransmite lo que corresponde al tercer y último nodo; éste vuelve a descifrar con su clave privada y envía ya la información a Internet. Por esta forma de trabajar, en la que hay varias capas de cifrado (como las capas de una cebolla) se le puso el nombre originalmente. Para el usuario todas estas operaciones están ocultas, y no es necesario ni siquiera saber que se realizan, pues basta con instalar un software de manejo bastante sencillo. En la Figura 3-21 puede verse el panel de control que permite acceder al registro de los mensajes del software, ver el ancho de banda que se está ocupando o cambiar el circuito por otro nuevo, con objeto de acceder a Internet desde otro punto remoto distinto (es lo que denomina "nueva identidad"). También se puede ver un mapa del mundo que muestra dónde están los puntos del circuito virtual establecido en cada momento (véase la Figura 3-22).

Figura 3-21: Panel de control de TOR

Adicionalmente al servicio de navegación, la red TOR permite el establecimiento de servidores dentro de la red y únicamente accesibles a los nodos que pertenezcan a la misma. Esta capacidad, junto con la resolución de nombres dentro de la red y con dominio propio, permite que cualquier usuario pueda configurar un servidor web, por ejemplo, que permanecerá oculto al grueso de usuarios de Internet que no estén integrados en la red TOR. La interacción entre servidores y clientes se lleva a cabo mediante "puntos de encuentro", de tal manera que el servidor no conoce la identidad de los clientes que se le conectan, y los clientes no pueden conocer la dirección IP de quien está proporcionando el servicio. Al servidor se le asignará una dirección consistente en una secuencia que no es fácilmente memorizable de caracteres alfanuméricos, y bajo el dominio ".onion". Las direcciones son algo similar a http://idnxcnkne4qt76tg.onion/ (ejemplo que corresponde al sitio web del proyecto TOR). La parte de la dirección antes del dominio tiene 16 caracteres y se deriva de la clave pública del servidor. Dada la popularidad de la red TOR, existen pasarelas para poder acceder, usando navegadores web sin ninguna configuración especial, a servidores de dicha red sin instalar el software de TOR; algunas de ellas son https://www.onion.to/ https://home.ayra.ch:4433/tor/ y http://tor2web.org/

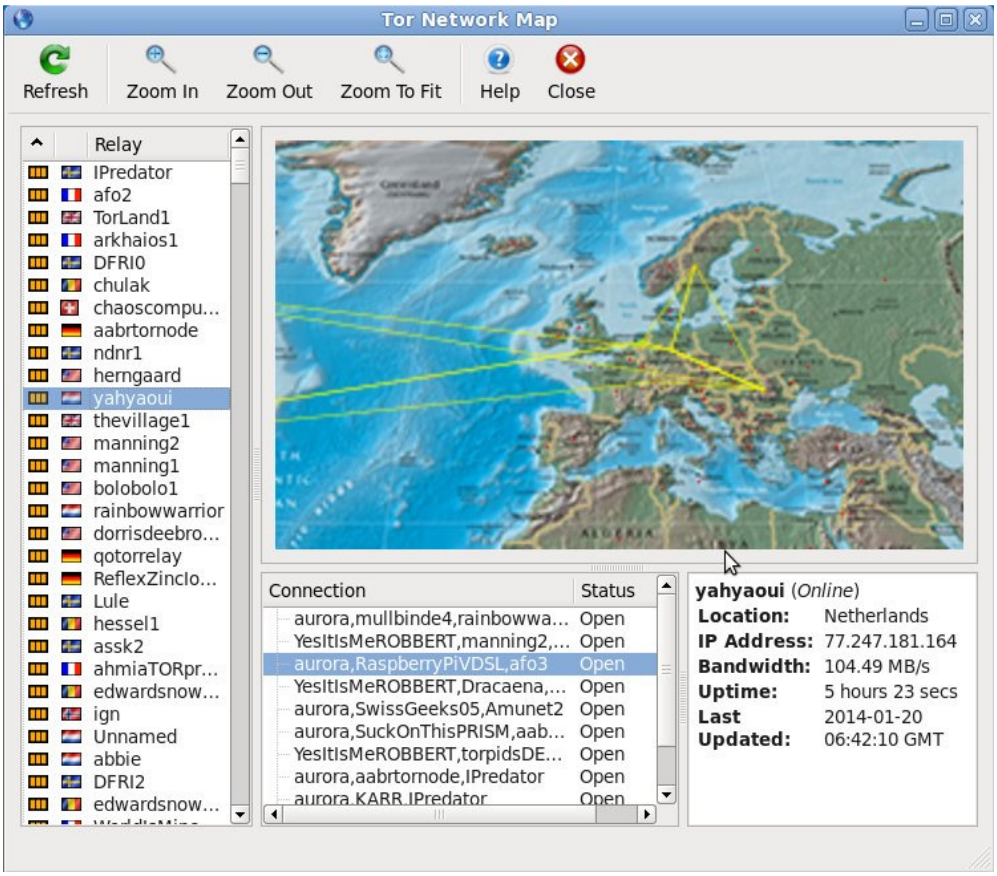


Figura 3-22: Mapa mundial con conexiones de TOR

Las distintas redes ocultas comparten algunas partes de su diseño y varios de sus objetivos, aunque difieren en algunos aspectos; así, TOR se basa principalmente en el anonimato en la red y en la posibilidad de provisión de servicios anónimos, pero no contempla el desarrollo de aplicaciones cliente propias, algo que sí hace I2P. Algunas tienen puntos en común; así, por ejemplo, es muy difícil conseguir el anonimato por completo, pues siempre se pueden seguir las pistas dejadas en servidores intermedios para llegar al originador de cualquier comunicación. Además, en las redes que se basan en el establecimiento de circuitos para “salir” a Internet por un nodo distinto del original, el último nodo de la comunicación tiene acceso a los datos “en claro” (o, al menos, a los datos que habría intercambiado el cliente con el servidor en caso de no utilizar una red oculta; si estos datos estuvieran convenientemente protegidos, por ejemplo por SSL, entonces no habría peligro de interceptación por parte del último nodo). También existen otros problemas añadidos, como el aumento del retardo en las comunicaciones finales, dado que todos los paquetes deben ser cifrados y descifrados varias veces, aunque, si la prioridad es el anonimato, el retardo puede no ser tan importante en primera instancia.

Ha habido otros proyectos, como Morphmix(152), JAP(153), Mixminion(154), AntsP2P(155) o MUTE(156), con funcionalidades parecidas a las indicadas anteriormente aunque sin un uso tan extendido.

La capacidad de establecimiento de servicios en redes ocultas junto con la de anonimato en la navegación, que impide que servidor y cliente se puedan identificar mutuamente, ha propiciado que el mundo del cibercrimen haya encontrado en las redes ocultas una herramienta perfecta para poder desarrollar sus actividades. Se pueden usar las redes ocultas para establecer foros de comunicación entre ciberdelincuentes, para vender y comprar productos ilegales (medicinas, drogas, armas, etc.), para adquirir software que sirva para la comisión de delitos (virus, troyanos, etc.), para contratar servicios relacionados con la ciberdelincuencia (campañas de *spam*, ataques dirigidos e incluso asesinatos), para comprar datos de tarjetas de crédito con objeto de cometer diversos tipos de fraude, etc. En la Figura 3-23 puede verse una página web en la que se vende droga. Esta página web está accesible dentro de la red TOR.

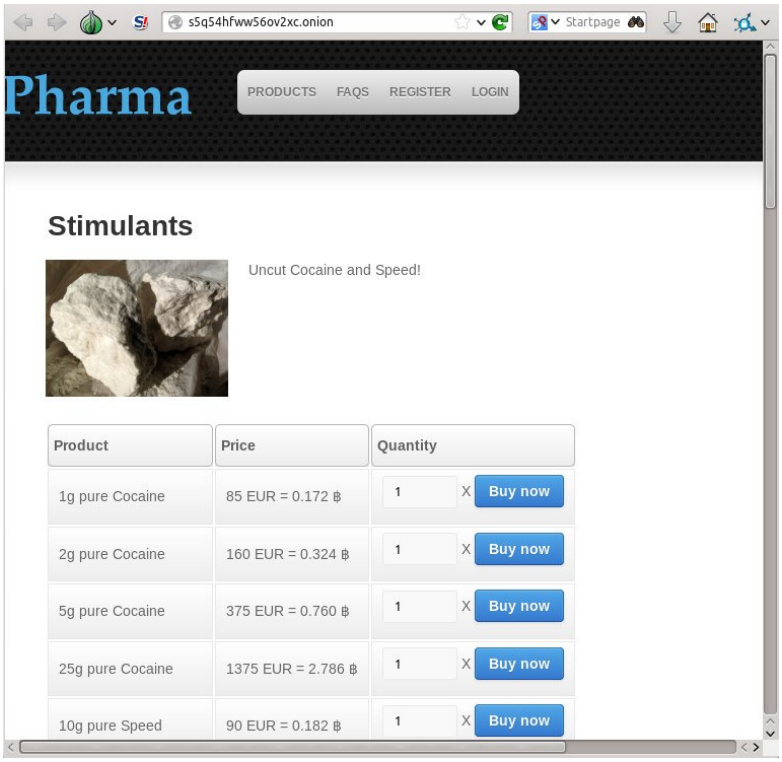


Figura 3-23: Venta de droga en web oculta

La Figura 3-24 muestra un servicio, dentro de la misma red TOR, de venta de pasaportes falsos del Reino Unido. De manera similar, en la Figura 3-25 se puede comprobar lo fácil que es conseguir licencias de conducir válidas en E.E.U.U.

Las fuerzas policiales realizan seguimientos de distintos sitios en el ciberespacio donde se realizan actividades ilegales, lo que frena en parte estas actividades delictivas. Como ejemplo, puede considerarse el cierre por parte de la agencia norteamericana FBI (*Federal Bureau of Investigation, Oficina Federal de Investigación*) de una red del mercado negro virtual de venta de medicamentos y productos ilegales y de otra de pornografía infantil(157)(158)(159).

Figura 3-24: Venta de pasaportes falsos en web oculta

Con lo explicado hasta ahora, no es extraño que con el tiempo el significado de la web profunda como conjunto de información no accesible a través de servicios de búsqueda ha ido evolucionando, y actualmente en muchos entornos se utiliza esa expresión para referirse al conjunto de comunicaciones y servicios que se mantienen fuera del alcance del usuario medio a propósito, con fines delictivos e ilegales en general.

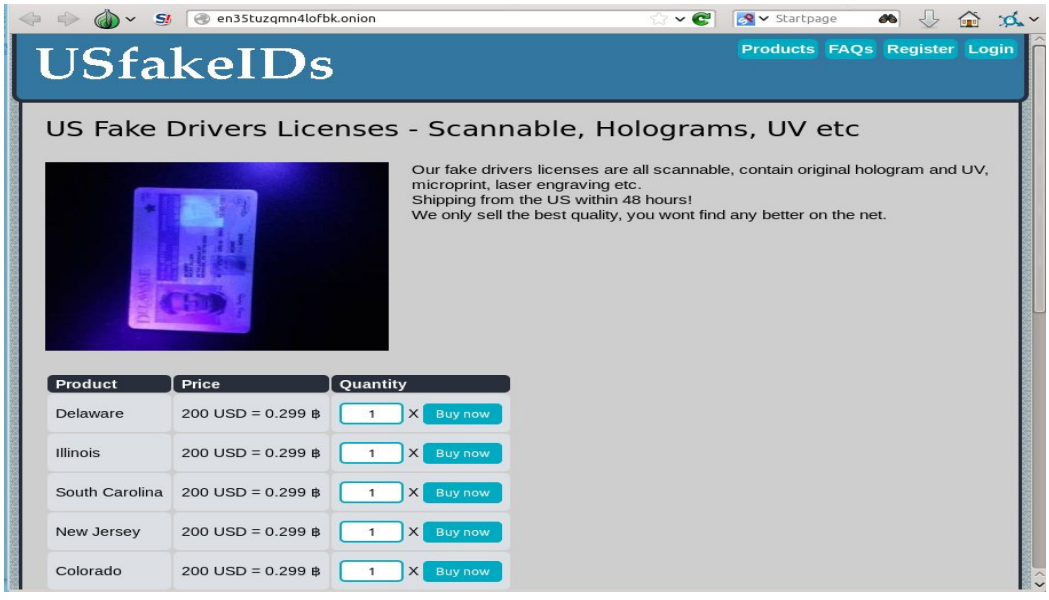


Figura 3-25: Venta de permisos de conducir falsos en web oculta

En otro terreno distinto al de las comunicaciones, aunque también desarrollándose en el ciberespacio, se encuentran las nuevas formas de monedas y pagos utilizando medios virtuales, como alternativas a los sistemas monetarios oficiales. Estas nuevas monedas son utilizadas por usuarios en general, pero también, cada vez más, por los cibercriminales.

El dinero que se suele manejar en la vida real es el llamado "fiduciario", denominado así porque se basa en la confianza o fe en el valor que tendrá en un futuro intercambio, y no se apoya en la equivalencia de la moneda con una determinada cantidad de metales o materiales preciosos o valiosos, como ocurría hace siglos cuando las monedas tenían el valor del metal con el que estaban fabricadas. El sistema monetario oficial se basa en emisores centrales de divisas, controlados por bancos, gobiernos e instituciones que determinan el valor y la equivalencia de distintas monedas en función de las circunstancias y de distintos intereses. En un intento de no depender de autoridades y sistemas bancarios centralizados y dirigidos, hay actualmente muchas iniciativas relacionadas con monedas virtuales, que solo existen en Internet y no tienen emisión de papel o de monedas físicas: es la llamada **moneda digital**, **criptomoneda** o **criptodivisa**.

Con las monedas digitales se pueden realizar pagos en todo el mundo, siempre que los proveedores acepten el pago en estas monedas; actualmente ya hay bastantes entidades y negocios, tanto físicos como virtuales, que lo hacen. Además los pagos se realizan directamente entre comprador y vendedor, sin necesitar entidades financieras intermedias.

Las monedas digitales suelen estar basadas en tecnología P2P, no dependiendo de autoridades centrales como ocurre con el dinero fiduciario. Dado que se exigen importantes requisitos en cuanto a la seguridad de los pagos y contra la falsificación, se basan en criptografía de clave pública. Habitualmente cada usuario dispone de una llamada "cartera virtual", que se crea en el equipo informático del usuario (ordenador o dispositivo móvil) mediante la generación de un par de claves (pública y privada) y que se identifica en el sistema y frente a otros usuarios por su clave pública. Cada vez que se realiza un pago se lleva a cabo una transacción (transferencia) entre dos carteras. Cada cartera virtual firma las transacciones en las que está implicada con su clave privada, y esta forma de firma digital autentica al usuario y las operaciones. La firma también sirve para evitar que se alteren posteriormente los contenidos de las transacciones, y en particular también permite comprobar la cronología de las mismas. Todas las transferencias realizadas se difunden entre los usuarios de la red de la moneda virtual en cuestión, y normalmente necesitan una confirmación en forma de consenso, que se produce unos minutos después de que se ordenen tras realizarse una serie de comprobaciones en la red. Tras la confirmación se produce la anotación de la transacción en el *block chain*, una especie de registro o libro de contabilidad público y compartido que almacena todas las transacciones e intercambios efectuados entre carteras virtuales. Este libro permite disponer de una memoria (o "histórico") que permite consultar las operaciones efectuadas y también comprobar el estado de todas las carteras virtuales, importante por ejemplo para estar seguro de que cuando un usuario quiere gastar una determinada cantidad de dinero, su cartera realmente tiene el

suficiente como para afrontar el gasto. Así pues, la posesión del dinero o de la cartera virtual por cada usuario se basa en la protección de su clave privada, y el dinero no se almacena en su dispositivo informático (pues podría estar expuesto a manipulación fraudulenta por los propios usuarios), sino que se dispone de información del contenido de su cartera de manera distribuida. Además las transacciones permiten un cierto grado de anonimato, pues en ellas no se identifica al comprador.

Hay distintos criptomonedas en circulación actualmente. Quizá la más popular hoy en día sea bitcóin[58] (conocida por su abreviatura: BTC). Otras también muy conocidas son Litecoin, Dimecoin, Fedoracoin, Quarkcoin, PeerCoin; en total actualmente se conocen cerca de 200 tipos[59].

Se puede obtener moneda digital de varias maneras. Una es mediante generación en equipos informáticos, en un proceso que se conoce como minado, minería o extracción (del inglés *mining*); para poder generar criptomoneda hay que competir con el resto de equipos de todo el mundo para solucionar un reto criptográfico, siendo el resultado un "bloque". Cada bloque encontrado se retransmite a toda la red, que lo valida antes de que sea finalmente aceptado. Ese bloque tiene un "premio" en forma de equivalencia en moneda virtual; en la red Bitcoin, por ejemplo, siempre será menor a 25 BTC, y además según pasa el tiempo el premio equivalente de cada bloque solucionado va siendo menor. A partir de ese momento hay que encontrar otra solución de complejidad mayor que la anterior, y así sucesivamente. Se ha diseñado cada moneda de tal manera que se genere un número elevado pero limitado de moneda a lo largo de un determinado lapso de tiempo; por ejemplo, en la moneda bitcóin se prevé que se generarán 21 millones en varias décadas. En cuanto a Litecoin (LTC), el límite son 84 millones. La cotización o equivalencia entre las monedas virtuales y las oficiales va cambiando constantemente; en el momento de redactar este Proyecto un bitcóin equivale aproximadamente a 700€[60]. Se puede consultar la equivalencia de monedas en multitud de páginas web dedicadas al asunto; en la Figura 3-26 se muestra una captura de una de ellas[61].

[58] Aunque el término “bitcóin” aún no ha sido incorporado al diccionario de la RAE, se siguen en este trabajo las recomendaciones de la Fundación del Español Urgente, Fundeu, escribiéndose por tanto bitcóin, plural bitcoines, y en mayúscula cuando hace referencia a la red, por ser un nombre de marca. Véase http://www.fundeu.es/recomendacion/bitcoin/

[59] Puede consultarse una lista de criptomonedas, con su estado actual en cuanto a volumen de dinero generado, equivalencia entre monedas virtuales y volumen de negocio en transacciones, expresado en dólares de E.E.U.U. en http://www.cryptocoincharts.info/v2/coins/info

[60] Se ha indicado un valor medio, pues la equivalencia entre monedas virtuales y monedas legales depende en cualquier caso del mercado donde se intercambien.

[61] Información extraída de http://dc-charts.com/chart_btc.php?cu=1

Figura 3-26: Evolución de la equivalencia entre bitcoines y euros

Existen otros métodos para obtener monedas virtuales; por ejemplo, en Canadá se montó el primer cajero que permitía cambiar dólares canadienses por bitcoines(160). Ya hay empresas que venden cajeros automáticos para intercambiar moneda virtual y moneda real(161). No obstante ésta no es la forma más habitual, pues hay otras, como comprarla en sitios de intercambio virtuales o bien a vendedores independientes. Ejemplos de mercados de intercambio de divisas son MtGox[62] y Bitstamp[63] para la moneda bitcóin. Otro ejemplo es el portal de Internet LocalBitcoins.com[64], donde se puede comprar y vender bitcoines mediante intercambios en efectivo o bien usando formas de pago online. En la Figura 3-27 pueden verse las formas de pago de que dispone esta web para los intercambios. De esta manera, cualquier usuario puede comprar una cantidad determinada de dinero virtual pagando su equivalente en su moneda local (euros, dólares E.E.U.U., etc.), y la cantidad comprada pasará a su cartera virtual. Este es el método que pueden aprovechar los ciberdelincuentes para blanquear dinero procedente de actividades ilegales, incorporándolo a la circulación de la moneda virtual que se puede emplear posteriormente para adquirir bienes o servicios, o bien para volver a obtener dinero de curso legal en otro mercado distinto. Es difícil perseguir esta forma de blanqueo de dinero, pues habría que realizar un seguimiento exhaustivo en todos los mercados de intercambio, y en cualquier caso tras un profundo rastreo puede seguirse el rastro del dinero, aunque no es fácil identificar a los dueños en el mundo físico. El mundo del cibercrimen utiliza también las monedas virtuales para conseguir dinero de otras actividades delictivas. En algunos casos, como por ejemplo

[62] https://www.mtgox.com/ Este banco digital se ha declarado en bancarrota a principios de marzo de 2014 debido a problemas de seguridad.
[63] https://www.bitstamp.net/
[64] https://localbitcoins.com/es/

con código dañino de tipo *ransomware*, los ciberdelincuentes aceptan el pago en monedas virtuales (es el caso de CryptoLocker, comentado en las páginas 60 y 72). Un ejemplo cercano del uso de dinero virtual para blanquear el procedente de actividades ilícitas se descubrió con el arresto de los autores del llamado "virus de la Policía" en España (162)(163).

Figura 3-27: Sitio web para comprar y vender bitcoines

3.7 GRUPOS DELICTIVOS CONOCIDOS

Son muchos los grupos organizados conocidos por realizar acciones delictivas en el ciberespacio. En muchos casos los propios grupos se dan a conocer mediante acciones concretas y por la reivindicación posterior. Esta dinámica suele ser habitual en actividades de ciberterrorismo y reivindicativas en general, pues precisamente lo que se busca es la popularidad del grupo y la publicidad de sus ideas. En otros casos, los grupos se descubren por parte de los organismos oficiales o empresas especializadas en seguridad que estudian los efectos de las acciones llevadas a cabo. Algunos de ellos tienen nombres definidos, pero esto no siempre es así, pues en una gran parte de casos su objetivo no es obtener publicidad, sino todo lo contrario: interesa realizar los delitos sin que se despierte mucha atención por parte de las agencias y organismos dedicados a perseguirlos. Hay también personas que, de manera individual, realizan acciones delictivas, bien para conseguir beneficios económicos, bien para proclamar algún tipo de idea (llevando a cabo, por tanto, algún tipo de *hacktivismo*).

Se describirán a continuación algunos de los grupos identificados en el ámbito del cibercrimen, ciberterrorismo, ciberespionaje y *hacktivismo*, así como algunas de sus acciones más conocidas.

Muchos de los grupos que realizan actividades ilícitas en el ciberespacio responden claramente a algún tipo de *hacktivismo*. En el mundo islámico hay varios de estos grupos, que de una forma u otra realizan reivindicaciones a favor del Islam y en contra del mundo occidental. Estos grupos son en general independientes, aunque muchos de

ellos se comunican entre sí y a veces colaboran en algunas acciones, dado que sus ideales son muy similares.

Uno de estos grupos es el **Ejército Electrónico Sirio** (SEA, *Syrian Electronic Army*), conocido desde 2011. Se caracteriza por apoyar pública y abiertamente al actual presidente de Siria, Bashar al-Assad. Para ello suele realizar acciones de ataque de distinto tipo contra sitios web relacionados con grupos de la oposición, gobiernos occidentales y medios de comunicación. Entre ellas han sido muy conocidas las ejecutadas contra algunas redes sociales como LinkedIn (relacionada con el establecimiento de redes de contactos laborales y de negocios), medios de comunicación como BBC Weather Channel, BBC News, The New York Times, Huffington Post y agencias de noticias como Associated Press y Reuters. Habitualmente los ataques consisten en acciones de *defacement* o en secuestro temporal de cuentas de Twitter. Algunas de ellas han ocasionado pérdidas económicas; tal es el caso de un *tweet* falso publicado el 23 de abril de 2013 (véase Figura 3-28) en la cuenta de la agencia de noticias Associated Press que indicaba que habían estallado dos bombas en la Casa Blanca y el presidente de E.E.U.U., Barack Obama, estaba herido. Esto provocó una caída de 145 puntos en el índice Dow Jones, y una pérdida momentánea en el índice bursátil Standard & Poor's 500 de 136.500 millones de dólares(164).

Figura 3-28: Tweet falso sobre explosiones en la Casa Blanca

Otro caso muy conocido de ataque realizado por el grupo SEA estaba relacionado también con el presidente de E.E.U.U. Hay una organización que apoya a Barack Obama, llamada *Organizing for Action*, que controla la cuenta de Twitter del presidente. Las publicaciones (*tweets*) en esta red social están limitadas a 140 caracteres, por lo que, cuando se quiere publicar un enlace muy largo, se suele utilizar algún servicio en Internet para abreviarlo. La organización de apoyo tiene una cuenta en un servicio de este tipo llamado ShortSwitch, y el grupo SEA consiguió entrar en la cuenta utilizada por la organización de apoyo a Obama (véase Figura 3-29). De esta manera hizo que un enlace existente en un *tweet* de la cuenta oficial del presidente Obama llevara a los usuarios a ver un vídeo de propaganda de 24 minutos publicado en YouTube por el propio grupo(165).

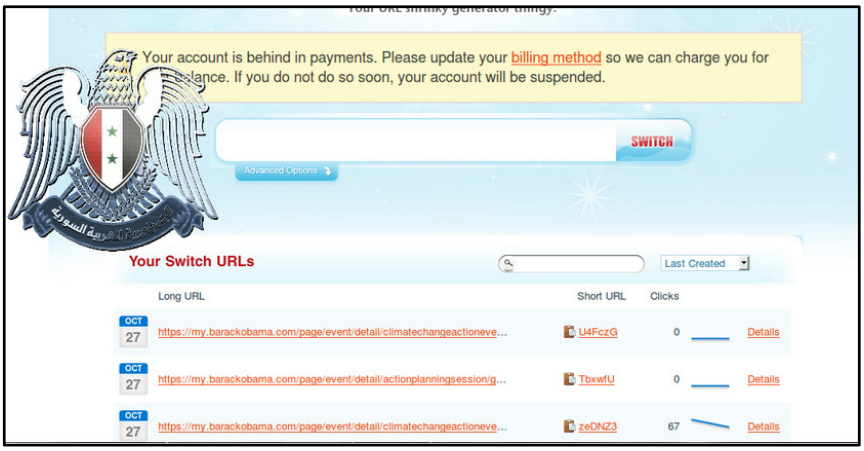


Figura 3-29: Demostración del ataque del grupo SEA

El SEA también logró apoderarse momentáneamente de la cuenta de Twitter del canal meteorológico de la BBC, BBC Weather Channel. En la Figura 3-30 pueden verse algunos de los mensajes publicados por el grupo sirio. En otro ataque que afectó al New York Times, cuando los usuarios intentaban acceder al sitio web del medio de comunicación, eran redirigidos a otros sitios propiedad del SEA; esto se consiguió por medio de ataques al sistema de resolución de nombres de dominio (DNS, *Domain Name System*).

Recientemente se ha llevado a cabo el último ataque del grupo SEA; en este caso, en los primeros días de 2014 tomaron el control del blog y de las cuentas en Twitter y Facebook del popular servicio de comunicaciones Skype, propiedad de Microsoft(166). Las cuentas intervenidas publicaron mensajes en los que se recomendaban que no se usaran los servicios de correo de Microsoft (ver Figura 3-31).

Figura 3-30: Ataque del grupo SEA a la cuenta de Twitter de BBC Weather Channel

Figura 3-31: Ataque del grupo SEA a la cuenta de Twitter de Skype

En línea con las ideologías del grupo SEA existe otro palestino llamado **KDMS Team**, del que se habló en la página 63, que ha protagonizado varias acciones en el ciberespacio. Los tipos de ataque que ha realizado principalmente son los típicos de las acciones de

protesta o publicidad, es concreto los de desfiguración en portales web; ejemplos de ellos son los portales del popular software de mensajería instantánea Whatsapp y de la empresa de seguridad AVG, en los que aparecieron en octubre de 2013 mensajes defendiendo a Palestina frente a Israel. Los ataques pudieron llevarse a cabo sobre la infraestructura DNS presumiblemente(167). Otras víctimas de este tipo de ataque realizado por este grupo y precisamente (y no por casualidad) en el entorno de la seguridad son el popular portal metasploit.com, las empresas ESET, BitDefender y AVG. Aunque los servidores web de tales objetivos no fueron comprometidos y solo se influyó en la infraestructura DNS, el alcance y la publicidad de las acciones fueron elevados, algo que suelen desear este tipo de grupos que protagonizan algún tipo de *hacktivismo*.

España no se libra de las acciones de grupos de protesta de los entornos islámicos. Hay uno, denominado **Moroccan Hackers Pro**, fundado en 2012, que ha atacado recientemente (año 2013) a varias webs españolas. En sus acciones reclaman la soberanía sobre Ceuta y Melilla y sobre el Sáhara. De igual manera, otro grupo marroquí, **Moroccan Islamic Union Mail**, ha realizado ataques a muchas webs españolas, la mayoría de negocios pequeños y medianos (autoescuelas, clínicas, un colegio de veterinarios, negocios de artesanía y otros). Los sitios atacados no son de gran relevancia de cara a obtener publicidad de sus ideas y reclamaciones. En realidad son varios los grupos marroquíes que últimamente están realizando sus acciones contra sitios web españoles, como Moroccan Ghosts, Virus-Noir, Réd-Sysanti, saw-19 y BilalSbXtra(168). Todos ellos suelen enviar los mismos mensajes, similares al mostrado en la Figura 3-32. En ocasiones puede haber contestaciones de otros grupos amenazando con represalias, como la que publicó en mayo de 2013 en YouTube el grupo Anonymous en respuesta a acciones de Moroccan Hackers(169).

Hay otros equipos que no son conocidos por grandes acciones, sino por haber aparecido en algún momento en las noticias, aunque sin quedar claro si realmente han realizado alguna operación. Es el caso de la llamada **brigada Abu-Nafsa**. Este grupo se atribuyó un supuesto ataque a la infraestructura crítica relacionada con la distribución de energía eléctrica en 2003 (ver página 33). Los estudios posteriores indicaron que fue el gusano *Blaster* el que provocó un fallo general en el enrutamiento de los equipos afectados. Falta saber si la propagación de ese gusano la inició la brigada Abu-Nafsa en una operación supuestamente llamada "*Quick Flash*" y ordenada por Ben Laden o si, simplemente, aprovechó la cobertura de una información importante para atribuirse tal acción y ganar popularidad.

Figura 3-32: Mensaje reivindicativo de un grupo islámico

En algunas ocasiones se encuentran actividades ilícitas que no pueden enmarcarse dentro de un entorno de protesta o bien de hechos delictivos con fines económicos. Suelen realizarlas grupos emergentes que, por alguna razón, no terminan de posicionarse y finalmente desaparecen. Tal es el caso de otro grupo que estuvo activo temporalmente, denominado **Q8 Army**. No está claro cuáles eran sus objetivos; realizaron algunas acciones relacionadas con publicaciones en varios sitios web de mensajes en torno a los ataques del 11 de septiembre de 2001 en E.E.U.U., pero su actividad se centró en robar datos de tarjetas de crédito con los que compraron ordenadores viejos y equipos de comunicación por satélite obsoletos. Entre 2005 y 2006 se sabe que consiguieron desplegar una *botnet*, a través de la cual instalaron distinto tipo de troyanos, *rootkits*, *spyware* y *adware*, aunque sin un fin claro. En su sitio web tenían una herramienta que permitía realizar distintas acciones como denegaciones de servicio distribuidas, envío de *spam* y campañas de *phishing*; también permitía cerrar automáticamente una sala de charla IRC. Disponían asimismo de un cliente de BitTorrent modificado para ser instalado en ordenadores de forma silenciosa; este cliente aceptaba posteriormente la descarga de películas piratas. La actividad cesó de repente, sin un motivo aparente. Se ignora si estaban probando herramientas para mejorarlas o implementarlas posteriormente, o si pretendían demostrar a otros grupos delictivos cuáles eran sus capacidades(170).

Un grupo que se ha hecho especialmente popular en todo el mundo es **Anonymous**. Realmente no se puede considerar como un grupo totalmente definido y con unas motivaciones, ideales y forma de trabajar uniformes. Más bien debe hablarse de una serie de grupos individuales, repartidos por todo el mundo, que actúan bajo un mismo nombre pero que se consideran "sucursales" en distintos países y entornos. Sus acciones son muy conocidas, por aparecer prácticamente de forma continua en los medios de comunicación no especializados. Lo habitual es que intenten realizar ataques de robo de información, desfiguración de páginas web y denegaciones de servicio. Para ello no suelen utilizar herramientas muy avanzadas, sino algunas técnicas simples como las de inyección de SQL. Además se da la circunstancia de que suelen avisar de las acciones que van a llevar a cabo, tanto en las redes sociales como en plataformas como YouTube. Por ejemplo, en 2012 se produjo una serie de ataques contra diversos sitios web de instituciones ecuatorianas como protesta contra una ley que establecía que los proveedores de servicios de Internet debían proporcionar información sobre la ubicación de los usuarios; estos ataques fueron avisados en YouTube el 1 de agosto(171); en abril de 2013 anunciaron un ataque contra Chile a causa de la construcción de dos centrales hidroeléctricas(172), y en noviembre del mismo año amenazaron con atacar 22 portales de Internet de Japón debido a la caza de delfines(173). Ya se han hecho famosas las frases utilizadas en la parte final de sus comunicados: "*Somos uno, somos todos. Somos Anonymous, somos legión. No perdonamos, no olvidamos. Espéranos*".

En sus acciones defienden algunas ideas comunes, como la libertad, tanto en el ciberespacio como en la vida real. En 2011 consiguieron acceso a varias cuentas de correo electrónico de miembros del gobierno de Irán; a continuación publicaron la información recabada (entre la cual se encontraban números de tarjetas de crédito y pasaportes) en la red BitTorrent(174). Poco después siguieron atacando a países considerados opresores en los que hay regímenes de gobierno dictatoriales, como Baréin, Egipto, Marruecos y Jordania. En esta operación, bautizada como *Revolution*, consiguieron acceder a las cuentas de correo de numerosos funcionarios(175). También avisaron al gobierno sirio tras dejar éste a sus ciudadanos sin acceso a Internet; el aviso se convirtió en acción en 2012, cuando el grupo atacó multitud de sitios web relacionados con el gobierno sirio(176). Previamente habían accedido al correo electrónico de varios asesores cercanos al presidente Bashar al-Assad(177). El mismo año 2012 se vio, en noviembre, otro ataque, esta vez a sitios web relacionados con el gobierno israelí, como protesta por el bombardeo previo en la Franja de Gaza(178).

En España Anonymous ha actuado varias veces. Una de ellas fue contra el sitio web de la Policía Nacional en junio de 2011, como respuesta por la detención de tres personas que supuestamente conformaban la cúpula de Anonymous en España(179). En el ataque a la web de la policía se usó la técnica de denegación de servicio distribuida(180). También ha habido amenazas por parte del grupo Anonymous al gobierno español. En agosto de 2013 difundió dos vídeos en el portal YouTube avisando de que iba a empezar la segunda fase de la llamada operación "*secret files*", que daría como resultado la publicación de documentos que demostrarían la implicación del gobierno y del partido

con el narcotráfico, además de probar influencias en entornos judiciales y policiales (181)(182).

Hay dos formas principales de proceder de este grupo; a veces actúan motu proprio para reivindicar alguna idea, y otras veces realizan sus acciones como respuesta a algún desafío. Este es el caso de la empresa de seguridad norteamericana HBGary, cuyo consejero delegado difundió en 2011 que iba a desenmascarar a los responsables de Anonymous(183). Como represalia, el grupo accedió a los servidores de HBGary, se publicaron multitud de correos electrónicos robados, se destruyeron muchos datos y se hizo un *defacement* del sitio web; además, otro sitio web propiedad del dueño de HBGary se dejó sin servicio, y se publicaron los datos de los usuarios registrados en él(184).

Aunque no es demasiado habitual, a veces los grupos organizados de protesta colaboran entre sí. Un ejemplo de ello es la colaboración de Anonymous con el conocido como **LulzSec** para atacar al gobierno de Brasil(185). Este grupo protagonizó otros ataques (a la NASA, al senado de E.E.U.U. y a Sony, entre otros). Finalmente cesó en sus actividades, tras publicarse los nombres del grupo, posiblemente por uno de ellos (Héctor Xavier Monsegur), que pudo haber sido fichado (o amenazado) por el FBI norteamericano.

También hay casos en los que los enfrentamientos trascienden y llegan al mundo real, con consecuencias terribles. En México, una banda criminal denominada Los Zetas(186) comenzó a asesinar en 2011 a personas que denunciaban sus acciones en Internet o tenían alguna relación con los sitios web donde se publicaban las denuncias(187). En esa campaña llegaron a secuestrar el 6 de octubre de 2011 a una persona, miembro de Anonymous. Este grupo disponía de nombres de colaboradores de la banda criminal, tras haber conseguido acceso a unos 25.000 correos electrónicos del gobierno mexicano. Aprovechando esa información, amenazó a Los Zetas con publicar detalles concretos de esos colaboradores de la banda, pertenecientes al mundo de la política y de las fuerzas de seguridad, entre otros, si no se liberaba al rehén antes del 5 de noviembre. La banda de Los Zetas contraatacó, intentando averiguar nombres de componentes de Anonymous para amenazarlos de muerte. Tras unos días de tensión, la banda criminal liberó al rehén el 4 de noviembre, aunque amenazó con matar a 10 personas inocentes por cada nombre de algún colaborador que Anonymous filtrara(188).

En general los grupos delictivos que se dedican a la realización de protestas o a la defensa de ideales políticos o religiosos suelen estar formados por ciudadanos que realizan tales acciones al margen de su vida particular habitual. En otros casos, se observa una manera de actuar tan meticulosa, exacta y organizada que podría pensarse en que los componentes del grupo son profesionales del ciberdelito. Sea o no sea así, estos grupos consiguen una efectividad en sus resultados que resulta sorprendente.

Existe un grupo, llamado **Hidden Lynx**, operativo desde al menos 2009 y considerado uno de los más activos y peligrosos. Realiza un trabajo de ataque en general, masivo, sin objetivo concreto, pero también ofrece servicios de ataque bajo pago, generalmente para obtener información específica de algún objetivo concreto. Tiene una alta capacidad de operación, pudiendo trabajar simultáneamente en varias campañas que se le hayan encargado; esto hace suponer que debe de disponer de un equipo humano de entre 50 y 100 personas. Suelen utilizar habitualmente dos herramientas para llevar a cabo sus trabajos: la conocida como *Backdoor.Moudoor* (herramienta de acceso remoto, adaptada a su vez de otra conocida como *Gh0st RAT*) y *Trojan.Naid*; esta última se ha usado por este grupo para ataques muy especiales de robo de información a objetivos de especial valor, habitualmente con la técnica *watering hole*. No son simples usuarios de herramientas fabricadas por otros cibercriminales, pues suelen modificar el *malware* utilizado para adaptarlo al blanco elegido como objetivo. Esto hace más difícil detectar sus acciones.

Los ataques llevados a cabo por este grupo se han originado normalmente desde máquinas en China. Los objetivos suelen estar en países occidentales; de hecho, E.E.U.U. acapara algo más de la mitad de los ataques sufridos. Por sectores, el 70% de las víctimas pertenecen a los campos de la educación, empresas TIC, sector financiero y organizaciones gubernamentales.

Uno de los ataques más conocidos realizado por el grupo Hidden Lynx tuvo como víctima a la conocida empresa de soluciones de seguridad Bit9. En julio de 2012 el grupo logró infiltrarse en algunos equipos de la empresa, robando uno de los certificados usados por Bit9 para firma de código. Esto les permitió firmar 32 ficheros con contenido malicioso, lo que les facilitó enormemente la comisión de posteriores acciones delictivas, dado que el robo del certificado no se descubrió hasta febrero de 2013. El certificado fue revocado, pero para entonces ya se habían realizado ataques con los ficheros firmados.

Otro caso bastante espectacular de ataque llevado a cabo por este grupo es la llamada operación VOHO. Usando la técnica de *watering hole*, se comprometieron servidores de 10 sitios web estratégicamente elegidos. En ellos se instaló distinto *malware* que logró infectar a casi 4000 equipos de usuario entre el 25 de junio y el 18 de julio de 2012. Los objetivos eran empresas y entidades oficiales de Washington y Boston, así como otras organizaciones implicadas en campañas para la democratización de determinados países. El *malware* instalado configuró una red APT que robaba información y la enviaba a un servidor de mando y control situado en Hong Kong.

Hay otros grupos que se dedican a actividades similares a las de Hidden Lynx. Es conocido que entre abril de 2011 y febrero de 2012 un grupo de origen chino llamado **Luckycat Hackers** realizó una serie de ciberataques a Japón, India y grupos relacionados con el Tíbet. Se trataba de una campaña APT cuyo objetivo era el robo de información en organizaciones relacionadas con la industria de la investigación en al ámbito militar, así como empresas de los sectores del transporte, energético y aeroespacial. En total

lograron comprometer 233 ordenadores, atacando a más de 90 objetivos. Curiosamente no utilizaba herramientas sofisticadas, pues ni siquiera desarrollaba ningún código que necesitara ser compilado, sino que utilizó lenguaje de *script* (en concreto *Visual Basic Script*, VBS), más fácil de manejar y más rápido para desarrollos simples. Además no utilizaron *malware* especialmente complejo para realizar la infiltración, aprovechando solo agujeros de seguridad básicos y técnicas de ingeniería social, y enviando correos electrónicos bien dirigidos y con una temática adecuada a los destinatarios. De hecho en el caso del ataque a Japón se aprovechó la confusión existente tras un gran terremoto y tras el desastre de la planta nuclear de Fukushima. Se enviaron correos relacionados con resultados de medidas de radiación nuclear, lo cual facilitaba que los ficheros adjuntos se abrieran por las víctimas, y aprovechando una vulnerabilidad del lector de documentos Adobe Reader se ejecutaban los *scripts* realizados. Éstos se conectaban a alguno de los 25 servidores de mando y control que se habían configurado, y recibían órdenes muy básicas pero suficientes para llevar a cabo las acciones deseadas (ejecución de comandos, envío y recepción de ficheros). Además la comunicación entre los equipos infectados y los servidores de mando y control se realizaba por el puerto 80 y con el protocolo HTTP, lo cual hacía que fuera fácil tratar con la infraestructura de *firewalls* de las redes de las víctimas, además de camuflar el tráfico entre el resto de comunicaciones relacionadas con la navegación web rutinaria.

Si se trata de hablar de algún grupo que realice robos de información a gran escala, no puede dejar de mencionarse al conocido como **Unidad 61398**, **Comment Crew**, **Shangai Group** o **APT1**. Corresponde a un equipo de trabajo que se considera parte del gobierno de China, activo al menos desde el año 2006. Varios estudios han conseguido localizarlo físicamente en un edificio de 12 plantas en el distrito Pudong de Shangai, y se da por hecho que el grupo está financiado y dirigido por el gobierno chino. Su trabajo es infiltrarse en gobiernos y empresas de todo el mundo para robar información de forma masiva, utilizando técnicas de APT. Según algunos cálculos podría haber robado cientos de terabytes de unas 140 organizaciones de todo el mundo. Inicialmente se le conocía en ámbitos oficiales de EEUU como "*Byzantine Candor*", aunque el nombre dejó de utilizarse al hacerse público tras la fuga de información publicada por WikiLeaks.

Las víctimas del trabajo de ese grupo han sido (y seguramente seguirán siendo actualmente y en el futuro) muy numerosas; se han identificado hasta ahora del orden de 140. Algunas pertenecen a entornos gubernamentales, como los Ministerios de Defensa y Exteriores de E.E.U.U. Otras están relacionadas con estos entornos, como empresas contratadas por la administración en relación con entornos militares, plantas químicas, compañías mineras y empresas de telecomunicaciones. También hay implicadas compañías que tienen relación con las infraestructuras críticas de E.E.U.U.: según un informe de la empresa de seguridad Mandiant(189), uno de los objetivos de la campaña es una empresa que dispone de acceso remoto a más del 60% de las conducciones de gas y petróleo en América del Norte. Entre otras informaciones robadas se encuentran procesos de fabricación de ciertas empresas, documentos con precios de productos, estrategias de negociación, datos de clientes e información tecnológica confidencial. A una sola de las víctimas, el grupo le sustrajo 6.5 TB en un período de 10 meses, lo que da idea de la capacidad de extracción del equipo y de la

efectividad de sus técnicas. Las intrusiones conseguidas son de larga duración, típica de las campañas APT; la media de tiempo de estancia en las distintas redes atacadas es de un año, durante el cual roban datos y contraseñas. En un caso concreto, el grupo estuvo infiltrado durante 4 años y 10 meses.

Algunas de las víctimas de gran nivel han sido Coca-Cola y la empresa de seguridad RSA. En ambos casos se realizaron ataques dirigidos, mediante el envío de correos electrónicos a determinadas personas, que siguieron un enlace a un sitio malicioso contenido en esos mensajes de correo, lo cual permitió a los atacantes infiltrarse en las redes privadas. Desde esos momentos, se robaba información que se transmitía a Shangai de manera semanal. El caso de RSA es especialmente importante, dado que esta empresa fabrica, entre otros productos, unos dispositivos o *token* de seguridad denominados SecurID, usados por agencias de inteligencia de EEUU, empresas contratadas por el Ministerio de Defensa y multitud de empresas importantes. Gracias en parte a la información conseguida de RSA por los atacantes, posteriormente éstos pudieron entrar en las redes del mayor contratista de defensa de EEUU, Lockheed Martin. Se cree que el grupo APT1 es el mismo que estuvo tras la llamada "Operación Shady RAT"(190), en la que se realizaron acciones de ciberespionaje a más de 70 organizaciones durante 5 años, entre las cuales están las Naciones Unidas y agencias gubernamentales de EEUU, Canadá, Corea del Sur, Taiwán y Vietnam.

En algunos casos los ataques no han tenido éxito desde el primer momento. Otra de las víctimas perseguidas por el grupo fue "Digital Bond", una pequeña empresa de seguridad especializada en equipos de control industrial. El ataque inicial consistió en un mensaje de correo electrónico dirigido a un empleado, que parecía proceder de su jefe. Redactado en un inglés correcto, el mensaje hablaba sobre algunas vulnerabilidades en sistemas de infraestructuras críticas, e invitaba al trabajador a seguir un enlace a otro documento. Éste no siguió ese enlace; se consultó a algunos investigadores, que descubrieron que el enlace dirigía al usuario a una herramienta de acceso remoto, y así se pudo abortar el intento de intrusión.

Otro caso de fracaso fue un ataque que podría haber sido el más peligroso, y que intentó penetrar en los sistemas de la compañía Telvent en Canadá. Esta empresa (en la actualidad propiedad mayoritariamente de Schneider Electric) diseña software SCADA para monitorización y control remoto de redes eléctricas y de distribución de energía, implicado por tanto en infraestructuras críticas. Telvent está presente y tiene acceso a más de la mitad de los sistemas de distribución de gas y petróleo de América del Norte y del Sur. Tras detectar que sus redes habían sufrido una infiltración y que se habían robado ficheros relacionados con diversos proyectos, Telvent avisó a sus clientes; el acceso se cortó, de manera que los atacantes no pudieron seguir robando información, pero las consecuencias podrían haber sido catastróficas si se hubiera empleado la documentación obtenida por los atacantes.

No siempre se encontrará en la escena del cibercrimen un grupo definido, compuesto por un determinado número de personas y quizá con un nombre. Existen también otras

entidades de mayor nivel que apoyan y posibilitan el cibercrimen. En este sentido ya se mencionó en el punto 2.3 (página 17) la red **RBN**, *Russian Business Network*. En un primer momento se constituyó como un proveedor de acceso a Internet, aunque su actividad derivó posteriormente hasta convertirse en su momento en el principal proveedor de herramientas y facilidades para el cibercrimen. Proporcionaba servicios de *hosting*[65] seguro para los cibercriminales, facilitando la dispersión de *malware* diverso, *phishing* y *spam*. Se consideraba que, aparte de proporcionar capacidad de almacenamiento de servidores, también participaba en la propia actividad delictiva activamente. Bajo su paraguas se llevaban a cabo multitud de acciones delictivas, incluyendo las relacionadas con pornografía infantil. Entre otras cosas se le conocía mundialmente por su distribución de *exploits* a través de antivirus y *antiadware* falsos, con los cuales conseguían realizar secuestros de equipos y robo de información. Operaba con diferentes proveedores de servicios de Internet, y bajo multitud de nombres de empresas distintas, todas en el entorno de Rusia y su periferia. Tuvo varias épocas en las que la actividad bajó notablemente, aunque luego resurgía. Su núcleo más importante dejó de funcionar en 2007, y durante los años posteriores distintos dominios que aún estaban activos se fueron desactivando por orden de ICANN [66] progresivamente(191)(192)(193)(194).

Por otra parte, en muchas ocasiones los protagonistas del mundo del cibercrimen no tienen nombres reconocidos ni tienen publicidad en sus acciones, salvo cuando son descubiertos o detenidos. Es el caso de una banda de 8 personas que han sido arrestadas en septiembre de 2013, acusados de robar 1'3 millones de libras esterlinas del banco Barclays. La forma de robarlo consistió en instalar, haciéndose pasar por técnicos de informática, unos dispositivos en un ordenador de una sucursal del banco[67]. Este aparato transmitía por radio la imagen del monitor y las pulsaciones de tecla del ordenador al que estaba conectado. De esa manera consiguieron los delincuentes datos de tarjetas de crédito y de cuentas bancarias de clientes, a los que les robaron dinero. La semana anterior se produjo un robo similar en una sucursal del Banco de Santander en Londres, y se cree que fue perpetrado por el mismo grupo(195)(196).

Se ha detectado en muchos grupos organizados anónimos que se dedican al fraude y al cibercrimen económico en general una organización similar a las estructuras mafiosas: existe una jerarquía interna muy estricta; hay distintos papeles jugados por personas con perfiles técnicos diferentes (*hacker* que penetra en los sistemas, personas que reciben la información personal robada y la vende, gestores que supervisan las operaciones y líderes o cerebros de las bandas), y no suele haber contacto directo entre ellos, ni siquiera conocimiento de la identidad de los integrantes de la banda entre sí.

[65] Almacenamiento de servicios en Internet (web, FTP, correo electrónico, etc.)
[66] ICANN es la Corporación de Internet para la Asignación de Nombres y Números (*Internet Corporation for Assigned Names and Number*), encargada de supervisar la asignación de identificadores de dominio en Internet, y asignar el espacio de direcciones IP.
[67] Instalaron un *switch KVM* para capturar la información de pantalla y teclado y un router 3G para transmitirla.

Esta similitud con organizaciones mafiosas y la forma de trabajo no son nada extraño, dado que en muchos casos los grupos que operan en el ciberespacio han estado delinquiendo en el mundo real, y han pasado al mundo virtual a la vista de las grandes posibilidades que éste ofrece. Para protegerse de posibles intervenciones policiales copian los procedimientos utilizados fuera del ciberespacio, con la ventaja de que en éste no es necesario el contacto físico para transferir información.

3.8 CONSECUENCIAS ECONÓMICAS DEL CIBERCRIMEN

Las principales actividades cibercriminales tienen habitualmente dos grandes objetivos: por un lado, defender y propagar ideas políticas, sociales, religiosas o de cualquier otro tipo: es el caso de las acciones de *hacktivismo*; por otro lado, se persigue como objetivo la obtención de beneficios económicos. Si bien las actividades de *hacktivismo* no tienen como principal móvil el económico, en ocasiones suponen pérdidas para las víctimas, en forma de credibilidad y, en algunos casos, por caída de ventas de productos o servicios. El resto de actividades, que sí persiguen obtener ganancias dinerarias, tiene una incidencia muy alta en la economía de ciudadanos, empresas, organizaciones y gobiernos.

Se puede decir que en general el cibercrimen es rentable para los delincuentes. No debe pensarse que los beneficios se han obtenido únicamente en una época muy reciente con la definitiva extensión de las nuevas tecnologías a todo el mundo desarrollado: ya en 2004, según la consejera del Ministerio de Hacienda estadounidense Valerie McNiven, la ciberdelincuencia facturó más dinero que el narcotráfico(197). Es difícil saber si esa afirmación es exacta, dada la naturaleza de ambas actividades, pero en cualquier caso da una idea de las consecuencias económicas del cibercrimen. De hecho, se estima que en 2005 las ganancias por el cibercrimen llegaron a ser el 1’6% del total de las transacciones de comercio electrónico en todo el mundo, sumando 2.800 millones de dólares de E.E.U.U.(198).

Aunque son muchísimos los datos que se pueden recabar respecto al dinero movido por el cibercrimen, valgan algunos datos sencillos como ejemplos. Según declaraciones de 2011 de la entonces detective superintendente británica Charlie McMurdie, encargada a la sazón de la unidad de cibercrimen de la policía metropolitana, la ciberdelincuencia costó al Reino Unido 27.000 millones de libras esterlinas en 2010(199). En aquella época el FBI norteamericano había desmantelado una banda de Estonia que había obtenido unos beneficios de 14 millones de dólares de E.E.U.U. tras infectar 4 millones de ordenadores de 100 países y obligarles a redirigir a los usuarios a ciertos anuncios publicados en páginas web. Prácticamente a la vez, un grupo de europeos orientales afincados en el Reino Unido fue detenido y condenado tras ganar unos 3’5 millones de euros robados de cuentas bancarias de ciudadanos particulares, utilizando el troyano Zeus(200). El autor o autores de Cryptolocker, código dañino mencionado varias veces en este Proyecto, podrían haber ganado, según diversas estimaciones, del orden de 41 millones de dólares de E.E.U.U. en medio año(201)(202)(203). Éstos son datos relacionados con las ganancias de los delincuentes con sus acciones ilícitas, pero

también hay cifras que hablan de pérdidas sin que intervengan beneficios: en 2009 se estimó que el gusano Conficker había causado pérdidas por valor de 9.000 millones de dólares tras haber infectado 3’5 millones de ordenadores(204). Estos datos permiten en conjunto acercarse al orden de magnitud de las cifras que se manejan en torno al mundo de la criminalidad en el ciberespacio.

De la información dada en el párrafo anterior se deduce que hay que distinguir entre los costes que suponen para empresas y organizaciones el haber sido víctimas de cualquier tipo de ataque y los beneficios que han obtenido los cibercriminales con sus acciones gracias a los robos y extorsiones a ciudadanos individuales. Para estudiar el primer caso existen informes realizados por empresas (habitualmente relacionadas con servicios de seguridad) que suelen realizar encuestas y estudios entre sus clientes para, a continuación, compilar los datos y ofrecer estadísticas. Para los segundos habría que realizar la misma encuesta con extensión mundial entre la ciudadanía que haya sido objeto de robo o estafa, y esto es bastante complicado. En su lugar, se suele acudir a las acciones policiales que consiguen detener a ciberdelincuentes, dando lugar a un estudio posterior de los medios utilizados, las cuentas bancarias disponibles, los movimientos existentes, los contactos con que contaban los ciberdelincuentes (socios, mulas, etc.) y otras informaciones de interés.

De cualquiera de las maneras es difícil calcular cuál es el coste económico de las acciones de los cibercriminales en todo el ciberespacio. Se producen pérdidas económicas por diversos conceptos: por delitos contra la propiedad intelectual, por fraudes bancarios con extracción directa de dinero de cuentas de usuarios y empresas, por pérdidas de mercado debidas a la caída de la confianza de los consumidores, por pérdida de credibilidad e impacto sobre la imagen corporativa, etc. En algunos casos muy concretos se puede conocer de manera prácticamente exacta cuál es la cuantía económica de las pérdidas de las víctimas de los ciberdelitos, o de las ganancias de los ciberdelincuentes; un ejemplo claro es el de los robos de credenciales bancarias o de datos de tarjetas de crédito o débito. En estas ocasiones basta con obtener datos procedentes de las entidades bancarias y de los propios usuarios para conocer qué cantidad de dinero ha sido sustraída de éstos. En otras situaciones, por el contrario, es complicado valorar lo que supone, en términos de términos de beneficios, cuánto han obtenido los ciberdelincuentes al cometer sus acciones, o bien, visto desde el punto de vista de pérdidas económicas, cuánto supone haber sido víctima del cibercrimen; piénsese por ejemplo en la destrucción de archivos en una determinada empresa, o el robo de esos archivos que, presumible pero no necesariamente, han podido ir a parar a manos de la competencia. En casos concretos como éste pueden aplicarse técnicas tales como prever cuántos productos se han dejado de vender y cuántos ha vendido la competencia gracias a la información robada, aunque en cualquier caso habría que sumar las pérdidas por el tiempo y los recursos empleados para diseñar y fabricar en su caso el producto que se considere y que no se va a vender como se presumía, aparte de posibles campañas publicitarias que pueden haber quedado sin efecto tras haberlas iniciado. También habría que incluir los gastos ocasionados por los propios ataques, que obligan a realizar investigaciones, implementar medidas para detener o mitigar el ataque en cuestión, obtener productos y servicios de seguridad, etc.

En algunos estudios de costes asociados al cibercrimen, en lo que concierne a ciberdelitos cuyas víctimas son las empresas y organizaciones, suelen dividirse las pérdidas entre costes directos (dinero empleado directamente para realizar actividades de denuncia, acusaciones legales, contratación de servicios de investigación y respuesta, adquisición de productos de seguridad o de servicios externos, y otros conceptos que suponen gastos inmediatos de dinero), costes indirectos (que contemplan el tiempo, el trabajo y otros recursos no directamente cuantificables) y costes de oportunidad (los que resultan de perder oportunidades de negocio, bajar las ventas y los ingresos, perder la imagen de marca, perder los beneficios que se hubieran podido obtener por campañas publicitarias previas y otros similares). Otra forma de realizar un análisis de costes consiste en considerar el coste de la infraestructura necesaria para prevenir ciberdelitos, el coste de las consecuencias de sufrir alguna acción, el producido por tener que dar una respuesta a los ataques (pago de indemnizaciones o compensaciones a víctimas, pago de tasas y a profesionales por asuntos judiciales, etc.) y finalmente los costes indirectos asociados (pérdida de reputación, pérdida de campañas publicitarias previas, pérdida en futuras ventas, etc.).

Cualquiera de las anteriores aproximaciones permite afinar en cierta medida los estudios de costes y particularizar el impacto de las distintas acciones que suponen sufrir un ataque de algún tipo. Los números obtenidos serán siempre una estimación y, por tanto, aproximados y no siempre reales, aunque al menos pueden aportar alguna cifra que indique de alguna manera el orden de magnitud de las pérdidas para la organización atacada. Muchas empresas dedicadas a los servicios de seguridad realizan estudios en este sentido, y dan algunos datos que, con la debida cautela, pueden ser analizados para ser conscientes de uno de los efectos, quizá el mayor, del cibercrimen en la economía mundial. Incluso con la incertidumbre de la exactitud de los datos obtenidos en los distintos estudios, éstos pueden valer a efectos comparativos, de tal suerte que se pueden comparar los números de distintos períodos de tiempo para estudiar la evolución de ciertos parámetros, o bien las cifras volcadas en estudios realizados simultáneamente en distintas área geográficas.

El Instituto Ponemon, especializado en realizar investigaciones independientes relacionadas con las tecnologías de la información y la protección de datos, ha realizado durante varios años un estudio del coste del cibercrimen en E.E.U.U., el último de los cuales se ha publicado en otoño de 2013(205). El estudio consiste en realizar encuestas a una serie de empresas de diversos sectores, entre otros de servicios financieros, tecnología, energía, defensa, educación, investigación, comunicaciones y el sector público. El número de organizaciones consultadas ha ido en aumento, siendo 45 en 2010, 50 en 2011, 56 en 2012 y 60 en 2013, lo que le va dando mayor credibilidad a los informes según pasa el tiempo. Además, por segunda vez se ha hecho el mismo estudio en Alemania, Reino Unido, Australia y Japón. En estos países no se tiene una larga referencia temporal de estudios anteriores, por lo que no cabe hablar de una perspectiva amplia en la evolución dentro de cada uno de ellos, pero sí es interesante realizar una comparación entre los distintos países en un mismo año, dado que entre todos los países involucrados el número de organizaciones es suficientemente elevado (concretamente 234).

De la información de E.E.U.U. analizada se pueden extraer algunas conclusiones y datos interesantes, que se exponen en los siguientes párrafos.

En el año fiscal 2013[68] el coste medio anual de pérdidas debidas al cibercrimen, para las 60empresas encuestadas, fue de 11'56 millones de dólares[69], con variaciones entre un coste mínimo de una de las empresas de 1'3 millones, y un coste máximo de 58 millones. Las acciones que más pérdidas ocasionaron fueron las denegaciones de servicio, los ataques de personal interno (incluyendo empleados internos, trabajadores temporales, contratistas y socios) y ataques basados en web.

Los costes estimados se pueden dividir en internos y externos. Los costes internos engloban la detección, investigación, respuesta, contención, recuperación y acciones posteriores. De todos estos conceptos, solo la detección y la recuperación ante incidentes ya suponen el 49% del total de costes internos. Los externos abarcan la pérdida de información, interrupción del negocio, pérdida de ingresos y productividad, daños en equipos, penalizaciones, costes judiciales, pérdidas en comercialización de productos y otros costes. En este apartado, la pérdida de información supone el 43% del total de costes externos, mientras que la interrupción del negocio y la pérdida de productividad suman el 36%.

Es interesante observar que el coste medio de pérdidas por el cibercrimen ha ido aumentando a lo largo de los cuatro años en los que se ha realizado el mismo estudio en E.E.U.U. En el año 2010 la media de pérdidas fue de 6'5 millones de dólares; en 2011 era de8'4 millones, en 2012 aumentó un 6% hasta llegar a los 8'9 millones y en 2013 subió un 26%, llegando a los 11'6 millones de dólares antes mencionados. También es conveniente mirar el coste mínimo que ha supuesto, pues si bien la media engloba a las 60 empresas consultadas y hay variaciones importantes entre ellas en los máximos, puede comprobarse que cualquier incidente de seguridad puede ser tremendamente costoso. En el caso del informe comentado, los costes mínimos considerados fueron 1 millón de dólares en 2010, 1'5 millones en 2011, 1'36 millones en 2012 y 1'3 millones de dólares en 2013.

El coste del cibercrimen es mayor en empresas con más trabajadores, aunque si se hace el cálculo de "coste per cápita", salen peor paradas las pequeñas empresas. Además, ciertos sectores suelen sufrir mayores pérdidas: es el caso de las industrias de defensa, energía, servicios públicos y financieros.

Se observa asimismo que el tiempo requerido para resolver incidentes de seguridad influye en el coste. Los tiempos de resolución de incidentes variaron entre menos de 1 día y 277 días. La media de tiempo que se tardó para contener los ciberataques fue de 32 días, con un coste medio de 1 millón de dólares durante este período. Si se combinan

[68] En E.E.U.U. el año fiscal abarca desde el 1 de octubre de un año hasta el 30 de septiembre del siguiente, y se identifica con el año en el que acaba el período. Por tanto, el año fiscal 2013 corresponde al período entre el 1 de octubre de 2012 y el 30 de septiembre de 2013.

[69] En adelante se empleará la expresión "dólares" para hacer referencia a dólares de E.E.U.U.

estos datos con el hecho de que la media de tiempo para contener ataques de personal interno es de 65 días, puede colegirse que estos tipos de incidentes son de los más costosos para las organizaciones. En este sentido, como se ha indicado antes, se ha hecho el mismo estudio por segundo año en Japón, Alemania, Australia y Reino Unido. En cada país fueron distintos los costes incurridos por los ataques, así como los tipos de ataques sufridos. Las empresas japonesas eran las que menos incidentes sufrieron por personal interno; esto puede indicar una gran influencia de los valores culturales en aquel país. Por otra parte, la importancia de los distintos costes varía entre países: para E.E.U.U. y Alemania la pérdida de información constituye el mayor porcentaje de pérdidas, mientras que para Australia y Reino Unido esa circunstancia le corresponde a la interrupción del negocio. Para las empresas japonesas tienen igual importancia, en cuanto a pérdidas económicas, la pérdida de información y la interrupción de las operaciones.

En otro estudio realizado por el mismo Instituto y publicado en 2012 titulado "*The Impact of Cybercrime on Business*" (Impacto del Cibercrimen en los Negocios)(206) se analizan distintas empresas de E.E.U.U., Reino Unido, Alemania, Hong Kong y Brasil; en él se facilitan datos que pueden ser interesantes en cuanto a comparación de distintos países durante el mismo período de tiempo. El coste medio de recuperación de un ataque oscila entre 298.000 dólares en Alemania y 107.000 dólares en Brasil. Lo escalofriante es que la media de ataques semanales que causan interrupciones de negocio está entre los 82 de Alemania (con 79 en E.E.U.U., muy cerca) y los 47 ataques semanales en Brasil; la media total es de 66 ataques semanales. En todos los casos excepto en Alemania la motivación principal de los ciberataques era el móvil económico, seguido del robo de información. En Alemania estaban a la par los motivos económicos y la intención de parar las actividades de las organizaciones atacadas. Para los profesionales de las TIC encuestados, la mayor preocupación era la pérdida de información importante y la interrupción del negocio; lo menos importante para ellos era la pérdida de la reputación y de la imagen de marca, además de los propios daños en los equipos. Posiblemente si los entrevistados hubieran pertenecido a algún otro departamento que no fuera el de TIC las respuestas podrían haber sido distintas en este sentido.

Lo que está claro es que, a la vista de los costes, es productivo para los ciberdelincuentes perpetrar sus delitos. Se pueden hacer algunos cálculos rápidos poniendo como ejemplo campañas de *spam*. Se puede poner en marcha una campaña de *spam* por una cantidad cercana a los 5.000 euros (comprar un *malware* adecuado puede costar 1.000 euros, y adquirir una red zombi para que envíe los correos, en torno a 4.000 euros). La red zombi puede infectar del orden de 2.000 ordenadores; si cada ordenador infectado envía en torno a 80.000 correos, en total circularían 160 millones de correos. Un anunciante puede pagar del orden de 0'2 céntimos de euro por correo, lo cual proporciona una ganancia de:

$$160.000.000 * 0'002 – 5.000 = 315.000 €$$

Si se invierten 5.000 € y se obtienen 315.000 €, se ha multiplicado la inversión por 63.

Este es un ejemplo de los números que podría hacer un cibercriminal, aunque hay variantes. En vez de adquirirse una red zombi se pueden contratar los servicios de una ya desplegada. En este caso el coste de envío de un millón de mensajes de *spam* está en torno a 150 dólares, lo cual supone un ahorro importante y una rentabilidad aún mayor. En otros casos se puede comprar alguna vulnerabilidad de día cero, por un precio de varios miles de dólares (a partir de unos 5.000 según una investigación de la empresa Forbes de 2012 (207)), y a partir de ahí construir alguna herramienta que la aproveche para amortizar la inversión, aunque en este caso se requiere tener conocimientos técnicos avanzados.

Otras herramientas permiten beneficios enormes a los cibercriminales. A principios de 2013 fue detenida por la Policía Nacional una banda de delincuentes que usaban el famoso "virus de la Policía" para obtener dinero. Se estima que este grupo manejaba del orden de 1 millón de euros anuales con sus acciones fraudulentas(162).

Las pérdidas ocasionadas por los cibercriminales, como se ha comentado anteriormente, son enormes. En fechas muy cercanas a la redacción de este proyecto, concretamente en diciembre de 2013, Microsoft[70] afirmaba haber desactivado la peligrosa red ZeroAccess(208). Según dos expertos en seguridad(209), la red no está realmente inoperativa, pues solo se ha desactivado el componente de la red que permitía realizar el fraude del clic. La estructura de mando y control, basada en comunicación P2P, sigue intacta, lo cual permite volver a enviar alguna versión distinta del componente desactivado y seguir controlando los zombis. En cualquier caso, lo interesante del asunto es que la mencionada red zombi produce unas pérdidas a los anunciantes de Google, Yahoo y Bing de 2'7 millones de dólares al mes.

Otro campo que produce pérdidas económicas enormes es el de los delitos contra la propiedad intelectual, incluyendo la piratería y la falsificación de bienes. Según un informe de la Cámara de Comercio Internacional del año 2011(210), en 2008 el valor de los productos falsificados con medios digitales estuvo entre 30.000 y 75.000 millones de dólares en los países miembros; para el año 2015 se estima que estará entre 80.000 y 240.000 millones de dólares. Se indica en el mismo documento que la Federación Internacional de la Industria Fonográfica (IFPI, *International Federation of the Phonographic Industry*) afirma quelas ventas anuales de música cayeron, entre 1999 y 2008, en una cantidad cercana a los 15.000 millones de dólares. La principal causa fue la proliferación de sitios donde compartir y descargar música en Internet. El valor de los archivos de música disponible en Internet estaría en torno a los 40.000 millones de dólares. En 2008 el número de archivos que se intercambiaron ilegalmente en todo el mundo podría estar en torno a los 40.000 millones.

[70] La desactivación de la red se realizó por la Unidad de Delitos Digitales de Microsoft en colaboración con el Centro Europeo de Cibercrimen (EC3), el FBI norteamericano y otras empresas, como A10.

En España, y según un informe de la consultora norteamericana IDC de 2010(211), la tasa de piratería en la música fue del 97,9%; la de las películas del 75,8%. En los videojuegos hubo un porcentaje de un 66,2% y en la literatura se estimaba una tasa del 43,5%. El valor total de los contenidos afectados por la piratería superó los 5.500 millones de euros. En un informe posterior publicado en2013y realizado por GfK(212) se indicaba el valor del lucro cesante para los contenidos pirateados el año anterior en distintos ámbitos: en la música era de 580 millones de euros, para el cine de 327 millones de euros, en los videojuegos la cifra se quedaba en 269 millones, y en los libros se estimaba en 45 millones de euros. El Estado pierde también ingresos por no percibir el impuesto sobre el valor añadido de los productos no comprados, y además, teniendo en cuenta la cantidad de puestos de trabajo perdidos por culpa de la piratería, habría que añadir lo que deja de percibir el Estado por estos puestos (seguridad social e IRPF); en total se estima una pérdida total en estos dos conceptos de 495 millones de euros.

Otros países han hecho sus propios análisis. En el Reino Unido se elaboró en 2011 un estudio del coste del cibercrimen encargado por la Oficina del Gabinete del Primer Ministro. Se estimaba entonces que la ciberdelincuencia le costaba al país 27.000 millones de libras esterlinas anuales, de los cuales 9.200 millones correspondían al robo de propiedad intelectual. A los negocios del Reino Unido le corresponden, en total, unas pérdidas de 21.000 millones de libras. El estudio incluía estimaciones de pérdidas debidas a fraude *online*, *scareware*, robo de identidad, robo de propiedad intelectual, espionaje, pérdidas de datos de clientes, robo *online*, extorsión y fraude fiscal. Los ciudadanos sufrirían, según el informe, unas pérdidas de 3.100 millones de libras al año, divididas en 1.700 millones debidos al robo de identidad, 1.400 millones por fraude en Internet y 30 millones por *scareware* y antivirus falsos. En Holanda un estudio realizado en 2012 indicaba que el cibercrimen suponía unas pérdidas a la sociedad de unos 10.000 millones de euros al año, aunque otros informes indicarían que más bien se encontrarían en el margen de 20.000 a 30.000 millones de euros; tres cuartas partes corresponden a las pérdidas para las empresas, el gobierno sufriría el 15% de ese coste y los ciudadanos el 10%. La mayor consecuencia correspondería al robo de propiedad intelectual, que supondría unas pérdidas de 3.300 millones de euros; el espionaje industrial estaría en segundo lugar con 2.000 millones de euros(213).

En definitiva, son muchos los estudios realizados respecto al coste que tienen los actos de ciberdelincuencia, y aunque, como se ha comentado, es difícil proporcionar datos exactos debido a la gran cantidad de factores que influyen, se puede deducir que se manejan cifras bastante elevadas en los distintos ámbitos analizados y en cualquiera de las zonas geográficas implicadas. El cibercrimen se ha convertido en un problema de primer orden, y se ha hecho necesario establecer todas las medidas legales posibles para combatirlo. El siguiente capítulo hablará de ello.

CAPÍTULO 4 POLÍTICAS Y ESTRATEGIAS DE SEGURIDAD. RESPUESTAS OPERATIVAS Y LEGALES

Ya se ha visto que las actividades del cibercrimen, el ciberterrorismo y el ciberespionaje están a la orden del día y que sus consecuencias, tanto económicas como de otro orden, son enormes. Se hace necesario establecer medidas legales efectivas para combatir tales prácticas, mediante la prevención y, en caso de que ocurran, la persecución de los correspondientes delitos. Estas medidas se materializan en forma de grupos de respuesta policiales, organismos de tipo gubernamental o similar (a nivel nacional e internacional), legislación específica e incluso creación de figuras judiciales especiales

para los asuntos tratados. Pero antes cada país debe haber establecido unas líneas de trabajo a corto, medio y largo plazo. En la práctica la mayoría de países con un desarrollo medio o alto en el uso de las TIC ha dictado ya unas "normas del juego" que suelen articularse en varios niveles, desde la esfera estratégica hasta la táctica u operativa.

En el primer y más amplio nivel se suelen encontrar las estrategias nacionales de seguridad. Son éstas documentos que definen las líneas estratégicas de trabajo de cada país en lo que a seguridad y posiblemente a defensa se refiere, a medio y a largo plazo. No solo tratan los temas relacionados con el ciberespacio; de hecho inicialmente no los trataban, pues tradicionalmente han contemplado aspectos relacionados con la propia identidad como nación, los intereses nacionales, el papel del país en el entorno político internacional y el bienestar de la sociedad, además de analizar las distintas amenazas como los desequilibrios sociales, los movimientos demográficos, las ideologías radicales, el cambio climático, la globalización y la prevención y respuesta ante catástrofes naturales. Los temas tratados en las estrategias nacionales de seguridad son de carácter amplio, y curiosamente el hecho de que se haya introducido en las últimas versiones de algunas estrategias la amenaza de distintos actores en el ciberespacio demuestra la importancia de éste en el funcionamiento de los países.

En un nivel inferior respecto a las estrategias nacionales de seguridad se encuentran las estrategias sectoriales concretas y las políticas que se deben seguir en ámbitos determinados, que suelen definirse más a corto y medio plazo. En lo que concierne a este proyecto, muchos países han publicado estrategias de seguridad de la información y de ciberseguridad. Otros publican políticas relacionadas con la defensa, en forma de "libros blancos" (es el caso de Francia), y si bien este ámbito parece no tener a priori relación con el cibercrimen, debe considerarse que las estrategias naciones contemplan los posibles casos de ciberataques y de ciberespionaje como amenazas a la seguridad nacional, de ahí que en los documentos relacionados con la defensa se tengan en cuenta las políticas de ciberdefensa. En cualquier caso, los documentos de este nivel suelen especificar pautas de actuación y también políticas concretas a seguir, incluyendo en muchos casos la creación o el refuerzo de grupos de lucha contra el cibercrimen (tanto policiales como de coordinación y ayuda para prevenir y combatir el cibercrimen) y la adaptación de la estructura penal y procesal, con modificaciones de la legislación penal vigente o la promulgación de nueva legislación, e incluso con la creación de fiscalías específicas.

Por otra parte ha habido en todo el mundo multitud de Iniciativas privadas nacionales e internacionales, asociaciones de empresas de diversos sectores industriales, conferencias promovidas por distintos foros públicos, privados y mixtos y disposiciones publicadas por muchos organismos realizando recomendaciones; se han realizado talleres, cursos, ponencias, seminarios y un sinfín de actividades en relación a la problemática de la ciberseguridad y con el cibercrimen como aspecto subyacente. Estas iniciativas no son objeto de estudio este proyecto, pues el objetivo del mismo es analizar las disposiciones y acciones realizadas en ámbitos institucionales oficiales.

En este capítulo se analizarán las estrategias de distinto tipo publicadas en países de todo el mundo, teniendo en consideración la evolución en el tiempo y sus contenidos, y dedicando un apartado especial a las publicaciones realizadas en el seno de los E.E.U.U., la Unión Europea y España. A continuación se hablará de las iniciativas existentes en cuanto a la creación de grupos operativos y de coordinación en la lucha contra el cibercrimen, tanto los materializados en forma de agencias internacionales como los integrados en las fuerzas policiales, así como los equipos de respuesta a emergencias. Por último se realizará un análisis de aspectos relacionados con el derecho penal, importante como parte final del proceso de lucha contra el cibercrimen.

4.1 ESTRATEGIAS DE SEGURIDAD, CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

Entrando en detalle en el análisis de las distintas estrategias, es interesante considerar cómo y cuándo han abordado los distintos aspectos de la seguridad diferentes países y organizaciones en todo el mundo. Para facilitar tal labor en el anexo I se pueden ver algunos de los documentos aprobados oficialmente relacionados con distintas estrategias, indicándose de qué tipo es cada uno de ellos y qué país u organización los ha publicado. El listado presentado no es exhaustivo, pues no se contemplan absolutamente todas las regulaciones aprobadas, ni tampoco todos los organismos de ámbito internacional que han redactado documentos al respecto, pero sí da una idea de la evolución y alcance en el tiempo de la preocupación de distintos países y organismos por la seguridad en el ciberespacio. Se puede observar que se contemplan estrategias de seguridad nacionales, y también otras relacionadas con el ciberespacio: respecto a estas últimas debe tenerse en cuenta que distintos países realizan aproximaciones diferentes a temas similares o relacionados, de tal manera que algunos definen estrategias de seguridad de la información y otros hacen lo propio con estrategias de ciberseguridad[71]. Estas diferencias de enfoque se deben en parte a las poco claras definiciones de ciertos términos, como se indicó en el capítulo 2 y se especifica incluso en algún documento oficial de los indicados (Ciberestrategia de defensa, Países Bajos). Como consecuencia, la temática tratada en los documentos referenciados no es uniforme. Así, no todos mencionan explícitamente el cibercrimen entre las principales amenazas; entre los que lo hacen se encuentran las estrategias de ciberseguridad de Australia, Alemania, Estonia, Finlandia, Noruega, Nueva Zelanda, Japón, España y Reino Unido, así como la estrategia nacional de protección ante ciberriesgos de Suiza. Tampoco es uniforme el tratamiento que se da a las infraestructuras críticas, estando en algunos casos ausente y en otros

[71]En ciertos casos se han contemplado aspectos de seguridad en otras políticas y documentos relacionados con la sociedad de la información en general, aunque suelen ser menciones sin demasiado detalle que precisamente hacen referencia a la necesidad de establecer disposiciones posteriores que contemplen la seguridad, que son las que se analizan en este trabajo. Un ejemplo es el documento de Finlandia de 2008 titulado "*The Information Society Policy Guidelines for the Association of Finnish Local and Regional Authorities*" (141). Estos documentos relacionados con la sociedad de la información no se han incluido en este estudio.

incluidas en mayor o menor medida en las estrategias analizadas, como las de ciberseguridad de Alemania, Austria, España, Estonia, Francia, Países Bajos, India, Nueva Zelanda, Japón y Suiza. Lo habitual en cualquier caso es contar con estrategias nacionales o disposiciones similares propias para las infraestructuras críticas, las cuales no se han incluido en el listado referenciado por tratar un tema muy específico que podría analizarse con mayor profundidad en otro estudio diferenciado. A este respecto es curioso comprobar que hay alguna estrategia como la de Austria (aprobada en 2013) basada directamente en la estrategia de seguridad nacional y en un programa de protección de infraestructuras críticas de 2008, aunque esto no es lo habitual.

En la elaboración de los documentos suelen intervenir distintos actores, tanto gubernamentales como académicos y privados, aunque suele haber alguna entidad oficial que es la que elabora y/o publica la estrategia finalmente. Un aspecto interesante relacionado con la diferencia de enfoques entre países es comprobar qué organismo realiza este papel en cada país. Así por ejemplo, se pueden citar las autoridades que han publicado algunas de las estrategias de ciberseguridad:

- Turquía (2013): Ministerio de Transportes, Asuntos Marítimos y Comunicaciones
- Países Bajos (2013): Ministerio de Seguridad y Justicia
- India (2013): Ministerio de Tecnología de la Información y la Comunicación
- Suiza (2012): Departamento Federal de Defensa, Protección Civil y Deportes
- Noruega (2012): Ministerios de: Justicia y Seguridad Pública; Defensa; Transporte y Comunicaciones; Administración del Gobierno, Reformas y Asuntos de la Iglesia
- Nueva Zelanda (2011): Ministerio de Tecnologías de la Información y las Comunicaciones
- Canadá (2010): Ministerio de Seguridad Pública
- España (2013): Departamento de Seguridad Nacional – Presidencia del Gobierno(214)

Las diferencias en este aspecto están motivadas en algunos casos por estar establecido así en los procedimientos del gobierno en cuestión o bien por estar implicados varios ministerios en los temas tratados, pero en otros interviene la distinta perspectiva que respecto a la ciberseguridad tiene cada país, influyendo, como se ha comentado, las diferencias en cuanto a definiciones de distintos términos. En este sentido es significativo que muchos de los documentos estudiados incluyen algún tipo de glosario o anexo con definiciones de términos (es el caso de las estrategias de ciberseguridad de Alemania, Austria, Finlandia y Nueva Zelanda entre otros); esto puede verse como una práctica normal en cuanto a aclarar los términos manejados en el documento, pero también como una forma de justificar qué enfoque se le ha dado a la estrategia en cuestión o qué organismo o ministerio dentro de la estructura gubernamental se ha encargado de la elaboración. Al hilo del asunto de los organismos que han elaborado las distintas estrategias es también interesante considerar la evolución que ha tomado la lucha antiterrorista en todo el mundo. Hasta hace unos años la persecución de terroristas era llevada a cabo exclusivamente por instancias policiales, por considerarse un problema que afectaba al orden y a la seguridad interiores de cada país. A raíz de los

acontecimientos terroristas en E.E.U.U. en 2001 y en Madrid en 2004, y con la internacionalización de los grupos y de las acciones ejecutadas, se ha visto una deriva hacia acciones militares encaminadas a impedir la organización de los grupos terroristas desde sus orígenes. Esta dinámica, unida a la obvia utilización de medios TIC por parte de las fuerzas armadas en todo el mundo, ha llevado a la situación actual en la que se mezclan o comparten las responsabilidades en lo que a ciberseguridad se refiere entre estamentos civiles y militares. No siempre se han establecido límites claros al respecto, aunque algunas estrategias sí lo hacen, como la de ciberseguridad de Austria, que indica claramente que las tareas de coordinación en caso de crisis relacionada con el ciberespacio se realizarán por el Ministerio Federal del Interior, aunque cuando se produzca un incidente de ciberdefensa en el que haya que proteger la soberanía en el marco de la defensa nacional se traspasará la coordinación al Ministerio Federal de Defensa y Deportes. En cualquier caso, los documentos referidos únicamente a la ciberdefensa no se incluyen en el anexo I por ser un tema muy específico, aunque sí aparecen documentos de defensa en general que contemplen la lucha contra el cibercrimen en alguna de sus facetas o que tengan alguna relación en su contenido con la temática de este proyecto.

Si se analiza la cronología de la tabla puede deducirse que las primeras preocupaciones por la seguridad en el ciberespacio surgen en los primeros años del siglo XXI. Son organizaciones internacionales las que comienzan a publicar documentos sobre la seguridad, alertando sobre la incidencia del cibercrimen: el Consejo de Europa publica en 2001 un Convenio sobre la Ciberdelincuencia que se constituirá desde entonces en referencia a nivel mundial para decenas de países (se analizará más adelante), y le acompañan la ONU, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico (APEC, *Asia-Pacific Economic Cooperation*) y la Organización de Estados Americanos. Tras estas organizaciones surgieron las regulaciones particulares de países individuales; entre los primeros que adoptan medidas al respecto se encuentran Rusia, E.E.U.U. y Reino Unido, aunque bajo el ámbito específico de ciberseguridad el primer país de la Unión Europea en publicar una reglamentación fue Estonia en 2008, tras los ciberataques sufridos en 2007. El análisis detallado y minucioso de la evolución de las distintas estrategias indica que, en general, puede decirse que hay dos grandes bloques que han ido a la cabeza en cuanto a la publicación y adopción de disposiciones relativas a la seguridad en el ciberespacio y a la lucha contra el cibercrimen: Europa y E.E.U.U. En estos entornos la evolución ha sido constante, aunque el resto de zonas del mundo no se han quedado atrás: Japón e India, junto con diversos países de África, han ido publicando sus regulaciones al respecto. En América los países que han ido en la vanguardia en este sentido son E.E.U.U. y Canadá. Llama la atención que la Organización de Estados Americanos (OEA) aprobara en 2004 una Estrategia Interamericana Integral de Seguridad Cibernética(215) y sin embargo el primer país latinoamericano en aprobar una estrategia de ciberseguridad lo hiciera ocho años más tarde, en 2011 (Colombia). Le siguió Panamá en 2013; otros países de este entorno, entre los que se encuentran Perú, Méjico, Chile y Uruguay están haciendo esfuerzos para disponer en breve de estrategias similares.

Otro detalle que puede observarse en la tabla del anexo I es que algunos países han renovado algunas de sus distintas estrategias en pocos años. Hay documentos que no indican un espacio concreto de tiempo durante el cual estarán en vigor, pero en otros el tiempo de validez se establece claramente, siendo habitual en estos casos considerar períodos en torno a los 5 años. Esto es debido a que el escenario del cibercrimen y las tecnologías cambian rápidamente, y es necesario realizar esfuerzos de adaptación normativa que no suelen ser fáciles, dada la habitual inercia de las administraciones y el tiempo necesario para estudiar, elaborar y aprobar reglamentaciones en muchos países. Teniendo en cuenta estas dificultades, es positivamente destacable que haya países que hayan promulgado estrategias nuevas en cortos espacios de tiempo; como ejemplo puede citarse Japón, que ha publicado estrategias relativas a la seguridad de la información en 2006, 2009 y 2010, además de posteriores documentos sobre ciberseguridad (uno en 2012 y dos en 2013); también Noruega ha publicado estrategias sobre la seguridad de la información (2003 y 2007) y sobre ciberseguridad (2012). En los Países Bajos se publicó una estrategia de ciberseguridad en 2011 que fue renovada tan solo 2 años después; lo mismo ocurrió en el Reino Unido los años 2009 y 2011.

Entrando en detalles respecto a las distintas estrategias estudiadas, es interesante su lectura atenta, pues así se pueden descubrir aspectos singulares y también otros más generales y comunes.

Las estrategias de ciberseguridad, aunque diferentes entre sí y, como se ha comentado, distintas en cuanto al enfoque con el que abordan el tema tratado, suelen tener algunos puntos en común. En general, es habitual encontrar la justificación de la necesidad de una estrategia específica en el campo de la ciberseguridad, analizando en algunos casos la situación actual del país y del ciberespacio en general, junto con las oportunidades que ofrece y los riesgos que presenta su uso; también suelen especificar aspectos de gobernanza general relacionados con la ciberseguridad, definiendo responsabilidades asignadas a distintos organismos nacionales; a veces definen objetivos en cuanto a capacidades que se deben alcanzar a nivel nacional para combatir el cibercrimen. Normalmente las estrategias especifican la necesidad de establecer un marco legal de colaboración en el que se incluya al sector público y al privado; prácticamente todas coinciden en afirmar que es imprescindible contar con entornos que favorezcan la colaboración público-privada, donde intervengan actores gubernamentales, académicos y empresariales. También es habitual que muchas de las estrategias traten aspectos como la necesidad de percepción del riesgo de los actores implicados en el ciberespacio, a saber: ciudadanos, empresas, gobiernos e instituciones, pues partiendo de una base de usuarios implicados con la seguridad es más fácil combatir las amenazas como el cibercrimen o el ciberterrorismo. En este sentido se proponen campañas de concienciación e incluso ejercicios periódicos. La creación o el refuerzo de organismos de control, coordinación y de respuesta a incidentes suele estar presente también en los documentos analizados, y en línea con este punto, también lo está la necesidad de

colaboración tanto interna como externa o internacional entre los grupos mencionados, con objeto de facilitar las investigaciones de incidentes y también los aspectos procesales. Otro aspecto tratado suele ser la capacidad de mantener los niveles de servicio en el ciberespacio y de recuperación ante incidentes graves de seguridad (conocida habitualmente como resiliencia).

En cuanto a la elaboración y al contenido, algunas estrategias son muy simples, limitándose prácticamente a establecer la aceptación por parte del gobierno en cuestión de la necesidad de abordar el tema de la seguridad en el ciberespacio, con muy breves análisis de amenazas y algunos objetivos muy generales, como la estrategia de ciberseguridad de Alemania de 2011 y la de Luxemburgo del mismo año. Otras estrategias, por el contrario, son bastante completas; un ejemplo es la de ciberseguridad de Austria, aprobada en 2013, que incluye un análisis de los riesgos y amenazas presentándolos en un gráfico bidimensional en el que contempla la probabilidad y las consecuencias de cada uno, marcándolos con colores para una rápida comprensión de la situación del riesgo (véase Figura 4-1).

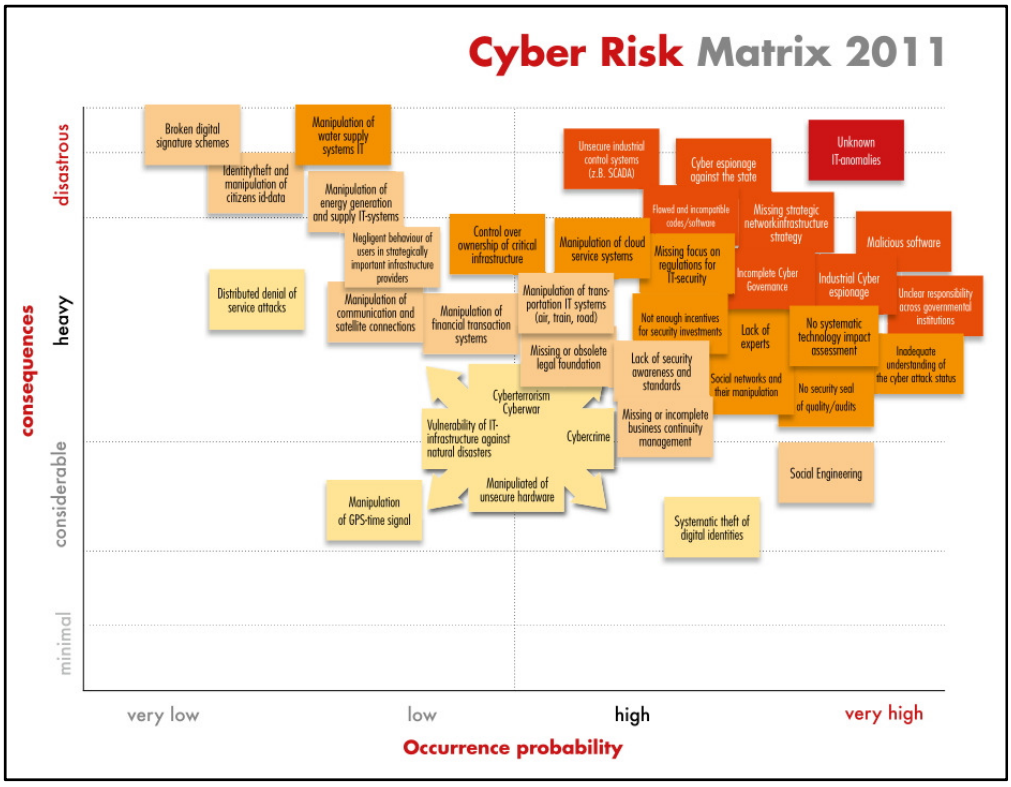


Figura 4-1: Matriz de riesgos de la Estrategia de ciberseguridad de Austria

La estrategia de ciberseguridad de Lituania es también exacta y exigente, pues llega a especificar una serie de indicadores y cuál debe ser el estado de los mismos durante los años de vigencia de la estrategia. En particular, indica qué valores tenían en 2011 y deben tener en 2015 y en 2019 algunos parámetros como: porcentaje de sistemas de información monitorizados, porcentaje de gestores de sistemas de información que han alcanzado un nivel de madurez adecuado, número de estudios de evaluación de las capacidades de ciberseguridad realizados, tiempo medio de respuesta ante

ciberincidentes y porcentaje de participación en eventos internacionales sobre ciberseguridad, entre otros. No solo especifica el valor de estos indicadores, sino que determina de manera clara y concreta qué institución o autoridad es la encargada de que se cumplan los objetivos establecidos.

También es muy detallada la estrategia nacional de seguridad de la información de Uganda. En este caso, contempla entre otras cosas descripciones detalladas de justificación, visión, misiones, objetivos estratégicos y líneas de actuación; análisis del estado actual del marco de la propia estrategia; análisis preliminar de riesgos internos y externos; marcos legales; referencias a investigación y desarrollo, concienciación, educación y formación; infraestructuras críticas; hitos importantes para cumplir los objetivos, etc. Además realiza un breve estudio de las regulaciones en materia de seguridad TIC de países de su entorno, en particular de Mauricio, Malasia, India y Emiratos Árabes Unidos. Esta práctica de hacer referencia a las disposiciones de otros países no es extraña; también aparece en la estrategia de ciberseguridad de Japón, donde se analiza la situación regulatoria al respecto en E.E.U.U., la Unión Europea, Reino Unido, Francia, Alemania y Corea del Sur. Otro caso similar es el de la estrategia nacional para la seguridad de la información de Eslovaquia, que indica que su elaboración se basó en un documento de la Unión Europea ("Una estrategia para una sociedad de la información segura - diálogo, asociación y potenciación", COM(2006) 251, ver página 137 para conocer el contexto en el que se aprobó), en la estrategia de seguridad nacional publicada tres años antes y en otros documentos estratégicos de países con sociedades de la información avanzadas como E.E.U.U., Alemania, Reino Unido, Finlandia, Japón, etc. aunque no especifica a qué documentos en concreto se refiere.

De manera complementaria al hecho de que algunos países se fijen en reglamentaciones de otros, existe también el caso contrario: los hay que indican claramente en sus estrategias que quieren ser referentes internacionales y estar a la cabeza en el ámbito de la ciberseguridad, como Japón y Finlandia. Esto puede interpretarse como una declaración de intenciones en cuanto a la seriedad y firmeza con que se aborda el tema tratado, pero también puede haber un componente económico al intentar dar la idea (tanto interna como externamente) de una situación de confianza de cara a trabajar con o invertir en ese país. En esta línea es particular el enfoque que se realiza en el Reino Unido, en el sentido de abordar la ciberseguridad como requisito importante para los negocios, con preferencia sobre otros ámbitos. Como prueba de ello puede consultarse la estrategia de ciberseguridad de 2011(216); tras analizar las amenazas (haciendo referencia a cibercriminales, ciberterroristas, actores estatales en forma de servicios de inteligencia y militares y, por último, *hacktivistas*), establece 3 secciones en cuanto a los sectores afectados, siendo la primera la dedicada a los negocios (las siguientes se refieren a la seguridad enfocada a las infraestructuras críticas y los individuos y sociedades). Más adelante, en el anexo dedicado a la implementación, se establecen varios objetivos por orden de prioridad, siendo el primero "*atacar el cibercrimen para hacer del Reino Unido uno de los lugares más seguros del mundo para hacer negocios en el ciberespacio*".

Continuando con la misma estrategia del Reino Unido, es interesante comentar un aspecto que no se encuentra en todas las demás analizadas: el de la necesidad de contar con profesionales de la ciberseguridad bien formados. El documento habla incluso de "*hackers* éticos" que puedan ayudar a asegurar la protección de las redes. En tal sentido establece la necesidad de contar con programas certificados de entrenamiento especializado, reforzar la formación postgrado para tener una base numerosa de expertos e incluso establecer un instituto de investigación en ciberseguridad con la ayuda de una de las agencias de inteligencia del Reino Unido, el GCHQ (*Government Communications Headquarters*, Cuartel General de Comunicaciones del Gobierno).

Como se ha indicado antes, es habitual que, al principio de las distintas estrategias, se trate de justificar la necesidad de las mismas. Además de mencionar las inmensas posibilidades que las nuevas tecnologías han traído y la dependencia del ciberespacio para la vida normal de los países, a veces se hace referencia a diversos incidentes ocurridos en el propio país o en otros de su órbita. Es el caso de Japón: tras la publicación en 2009 de su segunda estrategia de seguridad de la información, E.E.U.U. y Corea del Sur sufrieron ataques masivos por motivos políticos. Estos hechos mantuvieron en alerta a Japón por las posibles consecuencias que podían tener. Poco después, en la estrategia nipona de seguridad de la información publicada en 2010 se mencionaban dichos ataques en el sentido de que podían ser una amenaza a la seguridad nacional y, por tanto, requerían algún mecanismo de gestión de crisis para los casos en que se pudieran producir.

El caso de Japón no es el único en cuanto a mención de incidentes importantes en las estrategias. La de ciberseguridad de Estonia de 2008 también hace referencia a uno, aunque en este caso la víctima fue el propio país: en 2007 Estonia sufrió un gran ciberataque debido a motivos políticos. En la capital de Estonia, Tallin, existe desde 1947 una estatua, el "Soldado de Bronce", como homenaje al ejército soviético tras la victoria sobre el alemán en la Segunda Guerra Mundial. Entonces Estonia pertenecía a la U.R.S.S., aunque en 1990 se convierte en un país independiente. Desde entonces hay una parte de la población con simpatía hacia todo lo que tenga que ver con la órbita de influencia rusa, y otra parte con los sentimientos contrarios. En la primavera de 2007 el gobierno decide trasladar de forma permanente la estatua del soldado al cementerio militar, con objeto de poder realizar excavaciones en la plaza donde se encontraba anteriormente, en busca de restos de víctimas de la Guerra Mundial. Este traslado se interpretó como una ofensa por la población pro-rusa: se produjeron por ello manifestaciones y graves disturbios entre ambos sectores de población. Estos enfrentamientos tuvieron su continuación en el ciberespacio, pues desde el 27 de abril de 2007 hasta el 18 de mayo se llevaron a cabo ciberataques en distintas oleadas contra agencias gubernamentales, bancos, medios de comunicación y proveedores de servicio de telecomunicaciones de Estonia. Como consecuencia, Estonia, miembro de la OTAN

desde 2004, apeló al tratado atlántico y pidió ayuda a la Organización[72]. En un país como Estonia, fuertemente dependiente de las nuevas tecnologías, donde se utiliza Internet de manera extendida por toda su población para transacciones bancarias, trato con la administración, relaciones comerciales, etc.[73] el ciberataque tuvo consecuencias enormes(217)(218). Por este motivo no es de extrañar que en 2008 se publicara la estrategia de ciberseguridad de Estonia, firmada por el Ministerio de Defensa, que en el primer párrafo de su introducción mencionara los ciberataques sufridos el año anterior, considerados el primer ciberataque coordinado que se haya realizado contra un país. Tampoco es extraño que se mencione en el documento, en varias ocasiones, la necesidad de condena moral desde el entorno internacional a cualquier tipo de ciberataque, algo que no se observa en los documentos de otros países analizados.

En la estrategia de Estonia se observan diversas críticas en varios aspectos, quizá porque no pudo recibir la ayuda adecuada en el momento en el que lo necesitaba y sufrió las consecuencias sin poder defenderse ni actuar adecuadamente. Por ejemplo, dice, al referirse a las leyes internacionales, que no hay definiciones convenidas en cuanto a las amenazas existentes, en particular en lo que se refiere a los términos ciberguerra, ciberataque, ciberterrorismo o infraestructura de información crítica. Es interesante ver por otra parte que la estrategia no incluye medidas a nivel nacional para combatir el cibercrimen, pues para ello remite a la política penal del Ministerio de Justicia y al Ministerio de Asuntos Internos. Sin embargo, aun no incluyendo a propósito tales medidas contra el cibercrimen, se puede observar en la estrategia una serie de críticas al Convenio de Budapest, a pesar de haberlo ratificado con anterioridad a los ciberataques sufridos, concretamente en 2003. No solo hay críticas a este Convenio, sino también a una publicación de la Unión Europea (decisión marco 2005/222/JAI, ver página 137) sobre ataques contra los sistemas de información. Indica la estrategia que el documento de la UE, que básicamente sigue lo especificado en el Convenio de Budapest, solo se aplica a los países miembros de la propia Unión (de la cual Estonia es parte desde 2004), algo poco efectivo si se tiene en cuenta que el cibercrimen es un fenómeno que afecta a muchos más países. Otra crítica que le hace, aplicable también al Convenio de Budapest, es que trata los ataques contra los sistemas de información como delitos contra la propiedad pública o privada, no teniendo en cuenta la dimensión de seguridad nacional que puedan tener. Además indica que los sistemas informáticos se tratan todos por igual, sin tener en cuenta la diferencia entre los de uso general y los que están involucrados en infraestructuras de información críticas; como añadido afirma que no se distinguen entre ataques de pequeña y de gran escala.

[72] En la OTAN no existía experiencia previa con este tipo de situaciones. En octubre de 2007 los ministros de defensa de los países miembros reclamaron en su reunión la elaboración de una política de ciberdefensa, que fue adoptada en 2008.

[73] En 2007 el 98% de las transacciones bancarias se hicieron por medios electrónicos, el 82% de las declaraciones de impuestos se tramitaron a través de Internet, y se utilizaba ampliamente la firma digital tanto en entornos particulares como empresariales y oficiales.

De forma general, critica la estrategia estonia que los documentos de la Unión Europea no se centran en asegurar la ciberseguridad, sino que tienen como objetivo el mercado interno.

En cuanto al Convenio de Budapest, la estrategia indica que hay pocos países que lo hayan ratificado, pero que era significativo que varios miembros del propio Consejo de Europa (organismo que publicó el convenio) ni siquiera lo hubieran firmado, y mucho menos ratificado.

Precisamente la mención del Convenio sobre la Ciberdelincuencia o de Budapest es otro de los puntos en común de muchas de las estrategias analizadas. Aparte de las críticas al convenio que aparecen en la estrategia de ciberseguridad de Estonia, otros países lo mencionan en el sentido de indicar que lo han ratificado o bien para expresar que tienen intención de ratificarlo en el futuro. Entra las estrategias que hacen referencia al convenio están las de ciberseguridad de Alemania, Austria y la de seguridad de la información de Eslovaquia, país que ha traspuesto a su código penal las recomendaciones del convenio. Es interesante notar que países que no pertenecen al Consejo de Europa ni siquiera como observadores[74] y que se encuentran lejos de la órbita europea como Japón y Nueva Zelanda mencionen en sus estrategias de ciberseguridad el Convenio sobre la Ciberdelincuencia, el primero por haberlo ratificado en 2004 y el segundo por plantear en su estrategia a largo plazo la posibilidad de hacerlo.

4.1.1. E.E.U.U.

En E.E.U.U. la preocupación por una política uniforme en cuanto a la seguridad integral se acentuó a raíz de los atentados de septiembre de 2001. Poco después se publicó la Ley USA PATRIOT (véase página 31). Como parte de la estrategia general de seguridad nacional y entre las disposiciones posteriores que la completaban se encuentra la Estrategia Nacional para un ciberespacio seguro, de 2003. Varios años después, en 2008, se publicaba la Iniciativa Completa de Ciberseguridad Nacional (*Comprehensive National Cyber Security Initiative*, CNCI); un año más tarde se redactaba el documento *Cyberspace Policy Review* (Análisis de la política del ciberespacio). En ambos documentos la ciberseguridad se contemplaba como una de las mayores amenazas contra el país. Poco después, en 2010, se aprobaba la Estrategia de Seguridad Nacional, en la que las amenazas relacionadas con la ciberseguridad eran consideradas como uno de los retos más importantes a los que había que enfrentarse para conseguir niveles aceptables en cuanto a la seguridad nacional y el desarrollo económico. De acuerdo con esto, en 2011 se establecieron estrategias particulares para cada ámbito; en lo que concierne a la temática de este Proyecto, ese año se publica una estrategia con el título "*International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*" (Estrategia Internacional para el Ciberespacio – Prosperidad, Seguridad y Apertura en un Mundo Interconectado), en la que entre otros aspectos se incide en la economía, la

[74] En el momento de la redacción de este Proyecto los países observadores son Canadá, la Santa Sede, Israel, Japón, Méjico y E.E.U.U.

protección de las redes, la libertad en Internet, el cumplimiento de las leyes y la lucha contra el cibercrimen, incluyendo además aspectos militares aunque de manera escueta. También se publicó el mismo año el documento "*Cybersecurity, innovation and the internet economy*" (Ciberseguridad, innovación y la economía en Internet), por parte del Departamento (Ministerio) de Comercio. Otra disposición publicada el mismo año fue la Estrategia del Ministerio de Defensa para Operar en el Ciberespacio ("*Department of Defense Strategy for Operating in Cyberspace*"). También se publicó el documento titulado "*Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise*"(219) (Programa para un Ciberfuturo Seguro – La Estrategia de Ciberseguridad para la Iniciativa de Seguridad Nacional), en el que se proponían, entre otras, medidas para reforzar el ciberecosistema y proteger la infraestructura de información crítica.

El año 2011 fue muy productivo en lo que a publicación de disposiciones oficiales se refiere en el campo de la ciberseguridad. También apareció ese año el documento "*Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program*"(220)(Ciberespacio de confianza: plan estratégico para el programa I+D federal de ciberseguridad). Además ha habido multitud de programas nacidos a raíz de las publicaciones indicadas; a modo de ejemplo y como parte de las iniciativas indicadas en la CNCI para concienciación de la población respecto a la necesidad de seguridad en el ciberespacio, se puso en marcha un programa denominado NICE (*National Initiative for Cyber Security Education*, Iniciativa Nacional para Educación en Ciberseguridad). Otro documento que puede ser de interés, aunque no será analizados en profundidad, es "*Privacy Impact Assessment for the National Cyber Security Protection System (NCPS)*"(221) (Estudio de Impacto en la Privacidad del Sistema de Protección de Ciberseguridad), de 2012. Como se puede ver, en E.E.U.U. se ha publicado una gran cantidad de documentos oficiales relacionados con la seguridad en el ciberespacio, las implicaciones para la seguridad nacional, las políticas que se deben seguir y las líneas de actuación al respecto.

4.1.2. EUROPA

En el seno de Europa ha habido una constante preocupación por la lucha contra el cibercrimen y por la ciberseguridad en general desde hace muchos años. Ya en 1998 se publicó un estudio titulado "*Legal aspects of computer-related crime in the information society*" (Aspectos legales de la delincuencia informática en la sociedad de la información), más conocido como estudio COMCRIME, realizado por el profesor Dr. Ulrich Sieber, de la Universidad de Wurzburgo, y encargado por la Comisión Europea. En él se analizaba la situación de entonces, tanto en lo que se refiere a las vulnerabilidades encontradas como a aspectos legales, y se presentaban posibles pasos para el futuro y algunas recomendaciones específicas para la Unión Europea. Posteriormente ha habido una gran cantidad de documentos aprobados por dicho organismo, relacionados con los que anteriormente se han analizado del resto del mundo. Se incluye a continuación una lista con los más destacados al respecto, en la que no se han incluido los que tienen que

ver con lo relativo a la adaptación de la legislación penal, por tratarse más adelante en este trabajo. Se indica el año, título de la publicación y referencia oficial si la hay:

- 1998: Estudio COMCRIME sobre aspectos jurídicos de la delincuencia informática en la sociedad de la información
- 2000: "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" – COM(2000) 890
- 2001: "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo" – COM(2001) 298
- 2002: Directiva sobre la privacidad y las comunicaciones electrónicas - directiva 2002/58/CE. Incluye disposiciones contra el *spam* y el *spyware*.
- 2003: "Estrategia europea de seguridad: Una Europa segura en un mundo mejor"
- 2004: Reglamento por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) – (CE) 460/2004
- 2005: Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información
- 2005: "i2010 – Una sociedad de la información europea para el crecimiento y el empleo" – COM(2005) 229
- 2006: "Una estrategia para una sociedad de la información segura - diálogo, asociación y potenciación" – COM(2006) 251. Este documento fue la base para la estrategia de seguridad de la información de Eslovaquia de 2008.
- 2007: "Hacia una política general de lucha contra la ciberdelincuencia" – COM(2007) 267
- 2007: Tratado de Lisboa. Este documento modifica dos tratados principales anteriores, el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea. Este último pasa a llamarse Tratado de Funcionamiento de la Unión Europea. Lo importante a los efectos de este Proyecto es que se incorpora el concepto de una política europea (luego llamada "común") de seguridad y defensa (CDSP, *Common Defence and Security Policy*)(222). Se incluye una cláusula de defensa mutua entre naciones en casos de conflictos (artículo 222 de la versión consolidada del Tratado de Funcionamiento de la Unión Europea)
- 2008: se amplía la duración de la agencia ENISA – (EC) 1007/2008
- 2008: "Programa comunitario plurianual sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación" –Decisión 1351/2008/CE del Parlamento Europeo y del Consejo
- 2008: "Informe sobre la aplicación de la Estrategia Europea de Seguridad - Ofrecer seguridad en un mundo en evolución" – S407/08
- 2009: "Proteger Europa de ciberataques e interrupciones a gran escala: Aumentar la preparación, seguridad y resistencia" –COM(2009) 149
- 2010: Estrategia de seguridad interior de la Unión Europea: Hacia un modelo europeo de seguridad –5842/2/10
- 2010: nuevo reglamento para la agencia ENISA – COM(2010) 521

- 2011: se vuelve a prorrogar el funcionamiento de la agencia ENISA – (EU) 580/2011
- 2011: "Protecting children in the digital world" –COM(2011) 556
- 2011: "Cyber security: future challenges and opportunities" – informe de ENISA
- 2012: se publican los datos del eurobarómetro especial dedicado a la ciberseguridad, realizado en 27 países de la Unión Europea y en el que se analizan, entre otros parámetros, la frecuencia y tipo de uso que hacen los ciudadanos de Internet, su confianza en las transacciones electrónicas, su concienciación y experiencia con los cibercrímenes y su nivel de preocupación
- 2012: "Estrategia europea en favor de una Internet más adecuada para los niños" – COM(2012) 196
- 2012: "National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace" – informe de ENISA sobre estrategias de ciberseguridad
- 2012: "National Cyber Security Strategies - Practical Guide on Development and Execution" – guía publicada por ENISA
- 2013: se revoca el reglamento de creación de ENISA y se amplía su plazo de funcionamiento en 7 años, asignándole además funciones y regulando su funcionamiento – (EU) 526/2013
- 2013: "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro"
- 2013: "Concerning measures to ensure a high common level of network and information security across the Union" - propuesta de directiva de la Comisión con objeto de homogeneizar las medidas de seguridad de redes y sistemas de información en toda la Unión Europea – COM(2013) 48. Se realizó además un estudio de impacto (SWD(2013) 32)

Como se puede observar, ha sido muy abundante la publicación de normativas e informes en el seno de la Unión Europea, lo cual facilita que los estados miembros (e incluso los que no pertenezcan a la misma) puedan elaborar sus disposiciones a nivel nacional.

4.1.3. ESPAÑA

Las disposiciones legales publicadas en España merecen un estudio diferenciado. Para facilitarlo, en la Tabla 4-1 se indican varias de las aprobadas desde el año 2000 y consideradas de relevancia para este estudio.

En nuestro país la primera Estrategia de Seguridad Nacional vio la luz en 2011. Previamente no se había publicado ninguna, existiendo un cierto vacío en cuanto a las líneas de trabajo que se debían seguir en el aspecto de la seguridad nacional de manera integral. Ese vacío no existía en el entorno de la defensa, donde la reglamentación obligaba a publicar periódicamente determinadas Directivas de Defensa Nacional

(DDN) [75] y otros documentos internos del Ministerio de Defensa. Al no haber disposiciones legales fuera de este ámbito, se asumió en parte la responsabilidad de contemplar aspectos de la seguridad nacional por parte de este entorno; de hecho, en algunas de ellas se hacía referencia a la "seguridad y defensa" expresamente. Si bien es cierto que no en todas las DDN se contemplaban de manera exhaustiva los factores de amenaza nacional, también lo es que algunas de ellas trataban los temas propios de las estrategias nacionales de seguridad. Como muestra de ello puede consultarse la DDN 01/2008, en la que se realizaba un planteamiento estratégico donde se incluían asuntos que suponían amenazas para la sociedad en su conjunto, como el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva, los estados fallidos y el cambio climático. Sin embargo, la situación cambió precisamente tras la publicación de esta Directiva de Defensa Nacional, que establecía en su introducción lo siguiente:

> *(…) en línea con la tendencia general entre los países socios y aliados a integrar los objetivos relacionados con la seguridad de cada una de las políticas sectoriales en una estrategia nacional única, asegurando así su coherencia y coordinación, y sustituyendo la actual contribución interministerial a la seguridad y defensa por un enfoque más amplio e integral.*
>
> *La Directiva de Defensa Nacional se debe enmarcar, pues, en una Estrategia de Seguridad Nacional (…)*

Así, tres años después de la publicación de esta Directiva salía a la luz la primera Estrategia Española de Seguridad en 2011. A partir de entonces las publicaciones emanadas del entorno de Defensa volvieron a su ámbito particular, y las disposiciones relacionadas con la seguridad nacional se han hecho desde una perspectiva general e interministerial. Sin embargo no debe pasarse por alto la primera mención que se hacía de los riesgos existentes en el ciberespacio, en la mencionada Directiva de Defensa Nacional de 2008, que en su análisis del escenario estratégico indicaba:

> *La revolución tecnológica de la llamada 'Era de la Información' ha introducido una dimensión nueva en el ámbito de la seguridad y defensa, el 'ciberespacio', generando vulnerabilidades que pueden interrumpir o condicionar el normal funcionamiento de la sociedad.*

En el entorno general de la administración española ha habido otras disposiciones relativas a la seguridad en distintos ámbitos particulares. Como ejemplo, en 2010 se publicó el Real Decreto 3/2010 que regulaba el Esquema Nacional de Seguridad, con el objetivo de establecer una política de seguridad adecuada en el uso de medios electrónicos, proporcionando unos principios básicos y requisitos mínimos para obtener una protección adecuada de la información. Este esquema se había definido en la

[75] Se han publicado Directivas de Defensa Nacional en los años 1980, 1984, 1986, 1992, 1996, 2000, 2004, 2008 y 2012.

anterior Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos, estando pendiente la regulación específica que se aprobó en 2010. Sin embargo, de acuerdo con el objetivo de este Proyecto, no se consideran estas otras disposiciones por no estar enfocadas al establecimiento de unas estrategias de actuación en materia de ciberseguridad.

Año	Documento publicado
2000	Libro blanco de la defensa
2000	DDN
2003	Revisión estratégica de la defensa
2004	DDN
2005	Ley Orgánica de la Defensa Nacional 5/2005
2005	OM 37/2005 de planeamiento de la defensa
2007	Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos
2008	DDN
2010	RD 3/2010, Esquema Nacional de Seguridad en el ámbito de la administración electrónica
2011	Estrategia Española de Seguridad - "Una responsabilidad de todos"
2012	DDN
2013	Estrategia Nacional de Seguridad - "Un proyecto compartido"
2013	Estrategia de Ciberseguridad Nacional

Tabla 4-1: Disposiciones legales españolas relacionadas con estrategias de seguridad

Por tanto, desde 2011 España dispone de su primera estrategia de seguridad a nivel nacional; ésta, publicada con el título “Una responsabilidad de todos”, contemplaba el ciberespacio como uno de los escenarios en los que podrían aparecer amenazas, junto con el terrestre, el marítimo, el aéreo y el de la información. Admitiendo que las ciberamenazas podrían llegar a paralizar la actividad de un país, mencionaba también la operación de los grupos del crimen organizado y de los ciberterroristas en el mismo ámbito, lo cual lleva a la necesidad de disponer de una ciberseguridad adecuada para las infraestructuras vitales. La estrategia nació con una proyección temporal de 10 años, aunque ya especificaba que se revisaría cada 5 años o bien cuando las circunstancias lo aconsejaran. No hizo falta esperar tanto, pues tan solo 2 años después, en 2013, se aprobaba una nueva estrategia, esta vez con el nombre de Estrategia de Seguridad Nacional y llevando por título "Un proyecto compartido". Esta estrategia tiene carácter general, no estando centrada específicamente en la temática de este Proyecto. Sin embargo, como muestra de lo comentado al principio de este capítulo respecto a la necesidad de considerar aquí las estrategias nacionales de seguridad, se indican a continuación algunos aspectos considerados en ésta para poner de relieve la importancia de la seguridad en el ciberespacio dentro del ámbito general de la seguridad de nuestro país.

La introducción ya especifica que la ciberseguridad es uno de los principales ámbitos de actuación de la estrategia. De hecho en el capítulo 1, dedicado a indicar una visión general de la seguridad, ya se habla de los nuevos riesgos y amenazas, entre los que se encuentran los ciberataques, el espionaje, el terrorismo y el crimen organizado. El primer elemento es claramente una amenaza en sí misma; los otros tres se valen de distintos medios, entre ellos, como ya se ha comentado en este Proyecto, de las nuevas tecnologías y de las posibilidades que brinda el ciberespacio. Es significativo también que en el capítulo 2, en el que se identifican los entornos estratégicos de interés para España (Unión Europea, zona del Mediterráneo, América Latina, E.E.U.U. y otras zonas del mundo, junto con algunas organizaciones internacionales como la ONU y la OTAN) se indique que "*ya no es posible distinguir entre seguridad exterior e interior*". Esta afirmación es comprensible por los motivos indicados en el capítulo 2 de este Proyecto, entre otros, acerca de la facilidad con que se realizan actos delictivos y criminales en el ciberespacio. El capítulo 3 de la estrategia realiza un análisis de los riesgos y amenazas para la seguridad nacional, y se menciona el uso de las nuevas tecnologías como factor potenciador de riesgos y amenazas. Incluso en el apartado dedicado a los conflictos armados se habla del ciberespacio y del espacio exterior como ámbitos susceptibles de confrontación, en clara referencia a la necesidad de establecer medidas de ciberdefensa. Más evidente es la afirmación dada en un punto de este capítulo dedicado específicamente a las ciberamenazas, pues se indica que los "*ciberataques, en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo*" se constituyen en instrumentos de agresión a ciudadanos, empresas y organismos públicos y privados. También se comenta en el mismo punto la ausencia de legislación armonizada en ciberseguridad, algo que tendrá remedio unos meses después con la publicación de una estrategia específica para la materia. El espionaje en general, al cual se le dedica un punto específico del capítulo 3, brinda también la oportunidad de hacer referencia al aprovechamiento para tales actividades de las "*posibilidades de las TIC*".

El capítulo 4 de la estrategia define 12 ámbitos prioritarios de actuación; dentro de cada ámbito se indica un objetivo principal y distintas líneas de acción estratégicas, que definirán las actuaciones concretas que deban llevarse a cabo posteriormente. Uno de los 12 ámbitos es precisamente el de la ciberseguridad, y de las líneas de acción que se definen, unas son las habituales en las estrategias de otros países analizadas y otras son específicas del nuestro; algunas de ellas son:

- incrementar la capacidad de prevención y respuesta a ciberamenazas con el apoyo de un marco jurídico eficaz;
- finalizar la implantación del Esquema Nacional de Seguridad de 2007;
- mejorar la seguridad y la resiliencia de las TIC del sector privado, mediante el apoyo del sector público y la colaboración público-privada;
- promocionar la capacitación de profesionales en ciberseguridad;
- concienciar a ciudadanos, profesionales y empresas sobre la importancia de la ciberseguridad;
- aumentar la colaboración internacional en la materia.

Por último, ya en el ámbito organizativo, el capítulo 5 define un nuevo Sistema de Seguridad Nacional, compuesto inicialmente por un Consejo de Seguridad Nacional y Comités especializados que darán apoyo al Consejo. No se define ningún comité concreto, pues su creación y la asignación de funciones se harán en los respectivos reglamentos que se aprueben en su momento. No obstante, se indica que el Sistema de Seguridad Nacional se irá reformando y reorganizando paulatinamente, como de hecho se hizo meses después y se verá en los siguientes párrafos.

La Estrategia de Seguridad Nacional se aprobó en Consejo de Ministros el 31 de mayo de 2013; pocos meses después, el 5 de diciembre del mismo año, el Consejo de Seguridad Nacional aprobaba la Estrategia de Ciberseguridad Nacional. De esta manera España se ponía al día respecto al resto de países de todo el mundo que ya habían aprobado disposiciones similares anteriormente. Esta nueva estrategia surgía al amparo directo de la de seguridad nacional, y define de manera más concreta algunos objetivos específicos y líneas de acción determinadas. Se indica a continuación un resumen esquemático de su contenido.

El capítulo 1, "El ciberespacio y su seguridad", explica las características del ciberespacio y la importancia de la dependencia del mismo desde el punto de vista de la ciberseguridad; habla del incremento en el número de riesgos y amenazas, mencionando brevemente las características de los ciberataques. El capítulo 2, "Propósito y principios rectores de la ciberseguridad en España", tiene como finalidad fijar las directrices principales para un uso seguro del ciberespacio. En su breve exposición menciona la necesidad de la coordinación público-privada y la participación ciudadana, dentro del respeto a la Constitución y a las disposiciones de la Carta de las Naciones Unidas, de acuerdo con la Estrategia de Seguridad Nacional y "*en línea con otros documentos estratégicos nacionales e internacionales*". El capítulo 3 establece los objetivos de la ciberseguridad, y ya con mayor detalle, fija un objetivo global ("*Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques*") y 6 objetivos específicos para diferentes entornos, en concreto el de las administraciones públicas, el sector empresarial y operadores de infraestructuras críticas, el ámbito judicial y policial, en lo relacionado con la información y sensibilización, en materia de capacitación y en la contribución a la mejora de la ciberseguridad en el ámbito internacional. El capítulo 4 define las líneas de acción vinculadas a los objetivos antes expuestos. Por último, el capítulo 5 realiza algunas ampliaciones respecto a la estructura del Sistema de Seguridad Nacional que la Estrategia de Seguridad Nacional había creado. En particular, mantiene el Consejo de Seguridad Nacional, y además crea dos comités: el Comité Especializado de Ciberseguridad y el Comité Especializado de Situación; ambos actuarán de forma complementaria bajo la dirección del Consejo de Seguridad Nacional. En el primero se dará cabida a distintos departamentos, organismos y agencias de las Administraciones Públicas, aunque también podrán participar expertos del sector privado si se considera conveniente. No obstante, como es habitual en estos casos, los detalles concretos de su

implantación y puesta en marcha no se definen en la estrategia, quedando pendientes de la aprobación de posteriores disposiciones normativas y de reajuste, en su caso, de las existentes.

4.2 GRUPOS OPERATIVOS DE RESPUESTA

Una vez se dispone de una serie de estrategias de mayor y menor nivel que establecen las líneas maestras de la actuación contra el cibercrimen y las ciberamenazas, debe haber organismos del entorno operativo que implementen las medidas adecuadas. Estos organismos suelen ser, por una parte, agencias o estructuras similares que dan distinto tipo de apoyo a la sociedad y a los gobiernos; por otra, unidades o grupos de tipo policial que realizan el trabajo de campo y la investigación sobre el terreno para, finalmente, capturar a los cibercriminales y por último, equipos especializados de respuesta ante incidentes que suelen colaborar con los dos tipos de entidades anteriores de diversas maneras.

En nuestro continente existe un ejemplo del primer caso: la Unión Europea creó en 2004 la Agencia Europea de Seguridad de las Redes y de la Información, conocida como ENISA (*European Union Network and Information Security Agency*)(223), con los objetivos de servir de referencia para la seguridad en el ámbito de las TIC y dar apoyo a las distintas instituciones de la Unión Europea en la materia. En ese sentido facilita el intercambio de información, prácticas y conocimientos entre los estados miembros. Además participa en foros relacionados con la seguridad en las nuevas tecnologías en distintos entornos internacionales, aparte de participar en ejercicios de entrenamiento a nivel europeo e internacional y colaborar con diversos centros especializados de respuestas a incidentes (CERT/CSIRT, que se tratarán en la página 148).

En la esfera internacional, la organización INTERPOL[76], que trabaja con cuerpos policiales de 190 países repartidos por todo el mundo, dispone de unos grupos de trabajo denominados "*working party*" en Europa, América, África, Asia-Pacífico Sur y Latinoamérica. Estos grupos están formados por expertos que lideran las respectivas unidades nacionales contra los delitos informáticos. El G8 también dispuso la creación de la llamada *24/7 High Tech Crime Network* (red 24/7 de delitos de alta tecnología), que, aunque de tipo informal, proporciona puntos de contacto permanentes para intercambiar información sobre investigaciones de cibercrímenes. Se creó en 1997, y hay 45 países que pertenecen a esta red.

En la Unión Europea hay una agencia denominada EUROPOL(224) que proporciona asistencia a los estados miembros en materia de cooperación policial, tanto interna dentro de Europa como con países no miembros, como Australia, Canadá, Noruega y E.E.U.U. En el seno de EUROPOL se creó en enero de 2013 el Centro Europeo del

[76] El nombre oficial de la organización es ICPO–INTERPOL, por *International Criminal Police Organization*.La palabra INTERPOL viene de INTERnational POLice y era la dirección telegráfica desde 1946.

Cibercrimen, conocido como EC3 (*European Cyber Crime Center*)(225) para luchar contra el cibercrimen en la Unión Europea. Entre sus funciones están reunir y procesar información recogida por los distintos cuerpos policiales asociados, apoyar la investigación sobre el cibercrimen en la Unión Europea (tanto la realizada por países individuales como las que se realizan entre varios), realizar estudios de amenazas, tendencias y predicciones, apoyar la formación en la materia y promover la investigación y el desarrollo, trabajando con la sociedad civil, el sector privado y la comunidad universitaria e investigadora, equipos de respuesta a incidentes nacionales y el equipo de respuesta de la Unión Europea (CERT-EU), de los que se hablará más adelante. En el seno de EUROPOL se estableció en 2010 un grupo de trabajo para el cibercrimen denominado EUCTF (*European Union Cybercrime Task Force*), que agrupa a los responsables de las unidades de cibercrimen de los 27 estados miembros de la Unión Europea.

Ya en un nivel más operativo se encuentran las unidades policiales específicas para la lucha contra el delito en el ciberespacio. Las tareas de lucha contra el cibercrimen engloban muchas actividades. En general, para actuar se requiere disponer de alguna denuncia respecto a algún hecho considerado delictivo, aunque otras veces los cuerpos policiales realizan búsquedas activas sin denuncia previa buscando tales hechos. Una vez se dispone de una denuncia o conocimiento de posible ciberdelito, es necesario realizar una fase de investigación, que requiere habitualmente la recogida de información adicional y de pruebas efectivas, para que en la última fase se proceda a la detención (u orden de detención internacional si es necesario) y pase a disposición judicial de los supuestos delincuentes. Además de las labores habituales de investigación, recogida de pruebas y detención de criminales, suelen realizarse otras relacionadas con la colaboración externa con otros cuerpos u organismos, coordinación entre unidades subordinadas, formación dirigida a distintos ámbitos, asesoramiento a niveles políticos superiores (por ejemplo, para la elaboración de estrategias de más alto nivel), prevención y concienciación de los ciudadanos, entre otras.

Las unidades de tipo policial reciben distintas denominaciones en ocasiones. En general, y para simplificar sin entrar en detalles, suele hablarse de unidades de lucha contra el cibercrimen, pero en ciertos entornos se hacen distinciones en cuanto a las funciones concretas que se desarrollan. Así, se habla de “unidades de cibercrimen” para referirse a las que persiguen delitos contra sistemas informáticos y delitos que usan medios informáticos para su comisión, además de tener funciones forenses; es el caso de Francia y España. Las unidades relacionadas con “delitos de alta tecnología” son competentes para investigar delitos contra sistemas informáticos, teniendo asimismo cometidos forenses; este tipo de unidades se encuentra en Austria, Luxemburgo, Bélgica e Irlanda. Hay también “unidades forenses informáticas”, encargadas de la recogida de pruebas, como ocurre en Brasil. En este sentido, algunos entornos abogan por la separación entre las tareas de investigación y las de examen de pruebas, aunque esto no siempre es posible. Las llamadas “unidades centrales” tienen funciones de coordinación e inteligencia, no dedicándose a la investigación en sí.

En lo que concierne al emplazamiento orgánico de los distintos grupos policiales para combatir el cibercrimen, a veces se crean como parte de la organización de las estructuras ya existentes de los cuerpos de seguridad y otras veces se crean como organismos nuevos. En muchos casos la orgánica se va adaptando con el paso del tiempo, algo que es normal por otra parte, pues el primer impulso es crear, donde no lo haya, algún tipo de unidad especializada, y cuando esta unidad va creciendo en responsabilidades y en personal, se le suele reubicar o fusionar si es el caso. De acuerdo con esta dinámica, se ha podido observar que las distintas policías de todo el mundo van creando unidades nuevas o adaptando alguna de las existentes para combatir de forma más eficiente la nueva modalidad de delincuencia que las nuevas tecnologías han posibilitado. Así, por citar algunos ejemplos de varios continentes, en los Países Bajos existe la Unidad del Crimen de Alta Tecnología (*High-Tech Crime Unit*) del cuerpo de la policía nacional KLPD (*Korps landelijke politiediensten*). En Hong Kong las fuerzas policiales tienen una división del crimen tecnológico (*Technology Crime Division*). En Colombia existe el Centro Cibernético Policial (CCP), encargado de cuestiones referidas al cibercrimen y la ciberseguridad, con grupos dedicados a investigación contra el ciberterrorismo y la pornografía infantil en Internet, aparte de otros delitos. Dispone del llamado Comando de Atención Inmediata Virtual (CAI Virtual), un centro de atención con el que se puede charlar de manera interactiva en la página web del CCP(226).

Como se ha mencionado antes, hay casos en los que el funcionamiento de las unidades no se basa en esperar denuncias concretas, sino que se realizan tareas de prospección para tratar de localizar hechos delictivos. En Alemania, la Policía Federal Criminal (*Bundeskriminalamt*, BKA) dispone de un Centro de Servicios para Informática y Comunicaciones (227)del cual depende la Unidad Central de Búsquedas Aleatorias en Redes de Datos (ZaRD, *Zentralstelle für anlassunabhängige Recherche in Datennetzen*); este grupo realiza búsquedas continuas en Internet en busca de actitudes delictivas; en caso de encontrar indicios de delitos, prosigue con las consiguientes investigaciones, realiza la recolección de pruebas y remite el caso a la autoridad competente(228).

En otros países no existe una estructura nacional integrada y única para la lucha contra el cibercrimen. En India la solución implementada consiste en la creación de unidades aisladas en distintos distritos o ciudades; así, existe la Estación de Policía de Cibercrimen de la ciudad de Hyderabad, creada en 2010(229), o la Célula de Investigación del Cibercrimen de la policía de Bombay, creada el mismo año(230), que funcionan de manera independiente y sin estar integradas en una estructura de nivel superior que las coordine.

Hay países en los que ha habido más de un cuerpo policial dedicado a las mismas labores. En el Reino Unido la Policía Metropolitana creó en su momento la denominada *Police Central e-Crime Unit* (Unidad Central de Policía contra el Cibercrimen, PCeU) para combatir la ciberdelincuencia. Por otra parte, existía la denominada *SOCA Cyber*, rama de la Agencia del Crimen Organizado Serio (*Serious Organized Crime Agency*,) que también realizaba investigaciones y operaciones en el mismo campo. Ya en 2013 se creó la Unidad Nacional del Cibercrimen (NCCU, *National Cyber Crime Unit*)(231) como parte de la Agencia Nacional del Crimen (NCA, *National Crime Agency*), de acuerdo con lo

establecido en la estrategia de ciberseguridad de 2011. La NCCU engloba actualmente como parte de sus misiones las tareas realizadas por la PCeU y *SOCA Cyber*. Aunque la fusión no estuvo exenta de cierta polémica(232), es una muestra de que hay algunas intenciones de unificar esfuerzos en la lucha contra el cibercrimen en aras de conseguir una mayor eficacia.

E.E.U.U. es otro caso de proliferación de agencias e instituciones dedicadas a perseguir el cibercrimen. Allí se creó en 2002 el Departamento de Seguridad Nacional (DHS, *Department of Homeland Security*) tras los atentados de 2001. Este ministerio se creó a partir de 22 agencias federales ya existentes, con el objetivo de unificar todos los esfuerzos en seguridad nacional y con la misión, entre otras, de combatir el cibercrimen y asegurar las redes, constituyéndose en la "agencia líder" para los sectores TIC. Sin embargo, dentro del Departamento existen multitud de agencias que luchan contra el mismo objetivo. En el DHS existe la División Nacional de Ciberseguridad (NCSD, *National Cyber Security Division*), responsable de la gestión de riesgos, respuesta y ciberseguridad. También se encuentra integrada en el DHS la Oficina de Comunicaciones y Ciberseguridad (CS&C, *Office of Cybersecurity and Communications*), dentro de la cual se encuentra el Centro de Integración Nacional de Comunicaciones y Ciberseguridad (*National Cybersecurity and Communications Integration Center*, NCCIC)(233), con misiones relacionadas con la seguridad y la lucha contra el cibercrimen. Por otra parte el FBI, que está encuadrado también en el DHS, creó en 2002 la *Cyber Division* para combatir el ciberterrorismo, las operaciones de espionaje en el ciberespacio y el cibercrimen. Además opera el NCIJTF *(National Cyber Investigative Joint Task Force, Grupo de Trabajo Conjunto de Investigación Ciber*), que sirve como centro de solución de conflictos en las investigaciones entre 19 agencias federales(234). También dispone de las *Cyber Task Forces* (CTFs) desplegadas en sus 56 divisiones u oficinas de campo distribuidas por todo E.E.U.U. Tiene además unos equipos llamados CATs (*Cyber Action Teams*, Equipos de Ciber-Acción), compuestos por expertos en informática forense, *malware*, investigación de incidentes y seguridad informática en general, preparados para viajar en cualquier momento a cualquier parte del mundo para ayudar a resolver problemas relacionados con el cibercrimen(235). Hay incluso agencias como IC3 (*Internet Crime Complaint Center*, Centro de Denuncias de Delitos en Internet)(236), fundada por el FBI en colaboración con el NW3C (*National White Collar Crime Center*, Centro Nacional de Delitos de Guante Blanco), que realiza investigaciones y presta apoyo a instituciones estatales. Pero éstos no son los únicos organismos implicados en el cibercrimen: también lo está el llamado Servicio Secreto[77] (USSS, *United States Secret Service*), igualmente encuadrado dentro del DHS, que tiene una serie de grupos de trabajo conocido como *Electronic Crimes Task Force*s(237), además de un centro para realizar análisis forenses de terminales móviles en la Universidad de Tulsa(238). Fuera del Departamento de Seguridad Nacional también hay estructuras oficiales que realizan tareas similares. Por ejemplo, el Ministerio de Justicia (DoJ, *Department of Justice*) tiene una sección llamada CCIPS (*Computer Crime and Intellectual Property Section*, Sección de

[77] El Servicio Secreto se fundó en 1865 para evitar la falsificación de moneda.

Delitos Informáticos y Propiedad Intelectual), que realiza investigaciones relacionadas con el cibercrimen.

En España hay dos organizaciones en el seno de las fuerzas y cuerpos de seguridad del estado que realizan labores contra el cibercrimen: la Guardia Civil y la Policía Nacional. La Guardia Civil tiene el denominado Grupo de Delitos Telemáticos (GDT), encuadrado de la Unidad Central Operativa y creado en 1996 con el nombre de Grupo de Delitos Informáticos(239). Realiza una constante actividad de lucha contra el cibercrimen, además de dar consejos sobre el uso seguro de las redes de comunicación y medios informáticos. Dispone en todas las provincias españolas de los denominados Equipos de Investigación Tecnológica (EDITE), y para integrarse con los usuarios y facilitar la comunicación en ambos sentidos dispone de perfiles en redes sociales como Twitter (@GDTGuardiaCivil)(240), Facebook(241) y Tuenti(242), además de un canal en YouTube(243).

Por otra parte, la Policía Nacional tiene desde el año 1995 la Brigada de Investigación Tecnológica (BIT). Hasta hace poco estaba encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF), pero recientemente se ha creado la Unidad de Investigación Tecnológica (UIT), pasando la BIT a depender de dicha Unidad, junto con la Brigada Central de Seguridad Informática. La UIT es parte de la estructura de la Comisaría General de Policía Judicial, cuya organización puede verse en la Figura 4-2. La BIT realiza una labor activa de información a los ciudadanos para velar por la seguridad en el ciberespacio, además de la investigación de delitos relacionados con las nuevas tecnologías, teniendo como objetivo localizar y detener a los cibercriminales para ponerlos a disposición de la justicia. Al igual que el GDT de la Guardia Civil, tiene presencia activa en las redes sociales, con un perfil en Facebook(244). A un nivel más general la Policía Nacional tiene perfil en Facebook(245)y también en Twitter(246). Esta última cuenta (@policia) es conocida por el éxito que tiene dentro de la comunidad de esa red social; de hecho, en el momento de redacción de este Proyecto, la Policía Nacional es la primera fuerza policial en todo el mundo en número de seguidores, por delante del FBI norteamericano (@FBIPressOffice)(247). Este hecho es más significativo si cabe teniendo en cuenta la diferencia de población entre España y E.E.U.U.

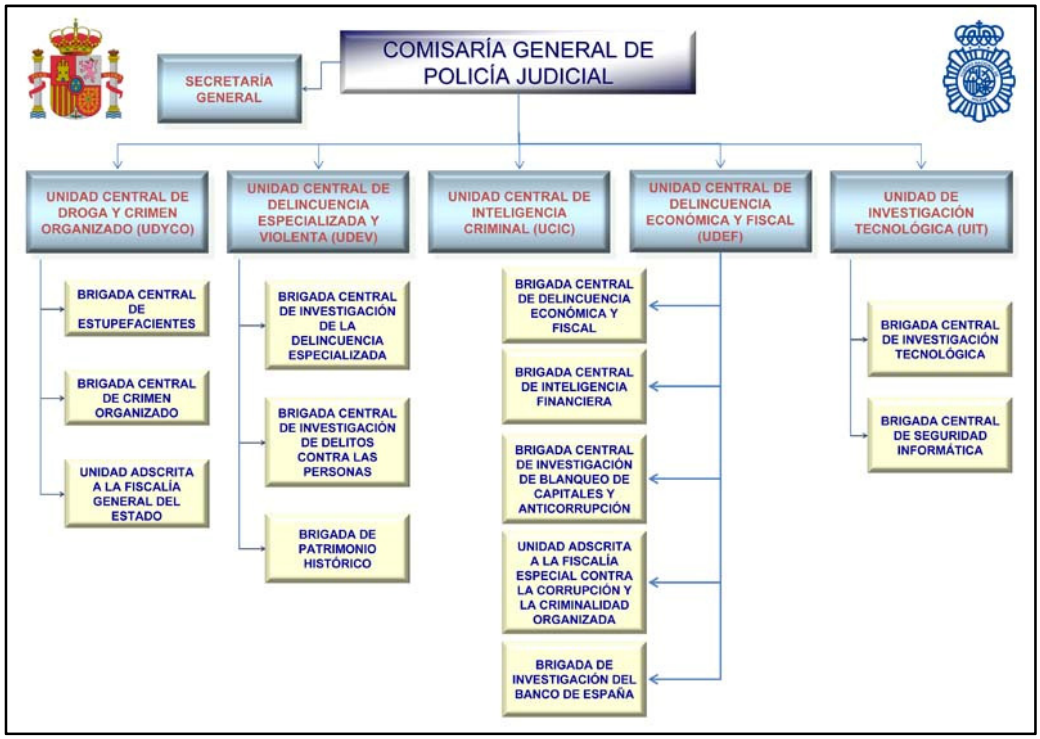


Figura 4-2: Organigrama de la Comisaría General de la Policía Judicial

Además de las organizaciones internacionales indicadas anteriormente y de los grupos operativos policiales dedicados al cibercrimen, existen otras estructuras que realizan importantes labores de apoyo y asesoramiento. Muchas de las estrategias relacionadas con la seguridad de la información establecían la creación de grupos de respuesta ante incidentes de seguridad, o la potenciación de los mismos en los casos en los que ya existían previamente. Estos grupos se suelen denominar CERT (*Computer Emergency Response Team*, Equipo de Respuesta ante Emergencias Informáticas) o bien CSIRT (*Computer Security Incident Response Team*, Equipo de Respuesta a Incidentes de Seguridad Informática) [78]. La misión de estos grupos está establecida en las reglamentaciones específicas de cada país, aunque en general suelen ser muy uniformes en todos, siendo generalmente de tipo preventivo y reactivo. Consisten en analizar constantemente el estado de amenazas en el ciberespacio, enviando y publicando alertas periódicas o extraordinarias; suelen realizar también labores de coordinación en la respuesta a incidentes, además de otras como campañas de información y concienciación dirigida a ciudadanos y empresas, realización de informes de seguridad general o relativos a amenazas concretas, asesoramiento en materia de seguridad dentro de su ámbito de actuación, colaboración con las fuerzas de seguridad en la investigación de incidentes y delitos y otras.

[78] El término CSIRT es de uso más general, ya que el acrónimo CERT es una marca registrada de la Universidad de Carnegie Mellon (159), que estableció el primer centro de este tipo denominado CERT/CC (*CERT Coordination Center*). Para que un centro pueda usar ese término debe solicitarlo a dicha Universidad. Puede consultarse una lista de los organismos autorizados a usarlo en la página http://www.cert.org/csirts/cert_authorized.html

Los CERT/CSIRT pueden ser de ámbito internacional, nacional o regional. Los hay de carácter oficial, encuadrado en algún organismo gubernamental o académico. También los hay de carácter oficial y transnacional; es el caso del EU-CERT, creado en 2012 para asistir a los distintas instituciones y agencias de la Unión Europea(248). Hay también muchos en el sector privado, tanto los propios de alguna empresa concreta como otros sectoriales que proporcionan servicios a una determinada industria.

En Europa prácticamente todos los países disponen de equipos de respuesta a incidentes. En España, de acuerdo con el sitio web de ENISA, hay reconocidos 15, algunos de organismos oficiales y otros del sector privado. De los que ENISA identifica como nacionales/gubernamentales, uno de ellos, operando desde 2007, es el del Centro Criptológico Nacional (CCN), encuadrado en el Centro Nacional de Inteligencia (CNI). Denominado CCN-CERT, elabora instrucciones y guías sobre aspectos diversos de la seguridad, ofrece soporte a distintos actores de las diferentes administraciones españolas (la general del Estado, las administraciones autonómicas y las administraciones locales), certifica la seguridad de los productos de cifra cuando así se requiere, acredita la seguridad de los sistemas y facilita constantemente información sobre amenazas y vulnerabilidades presentes en el ciberespacio. Otro CERT muy conocido y activo es el del Instituto Nacional de Tecnologías de la Comunicación, S.A., (INTECO), sociedad dependiente del Ministerio de Industria, Energía y Turismo, llamado INTECO-CERT. Éste está más enfocado a los servicios relacionados con los ciudadanos, la red académica y de investigación (RedIRIS) y empresas, realizando labores de fomento de la seguridad y de las buenas prácticas, además de realizar diversas acciones en materia de concienciación en aspectos diversos de la seguridad. En el entorno académico, el IRIS-CERT tiene como objetivo principal la protección de la Red IRIS y la red académica y de investigación nacional.

No son muchos los países de África que cuentan con equipos de respuesta. Entre ellos se pueden citar el KE-CIRT/CC (*Computer Incident Response Team/Coordination Centre*)[79] de Kenia, instaurado en colaboración con la UIT(249)(250). También hay otros como el maCERT de Marruecos, el ECS-CSIRT de Sudáfrica, el EG-CERT de Egipto y el tunCERT de Túnez.

En América son muy numerosos los países que han creado equipos de respuesta a incidentes: en E.E.U.U. hay muchísimos (varias decenas), de entre los que se pueden citar CERT/CC y US-CERT; en Canadá hay también bastantes, entre los que está el gubernamental *Canadian Cyber Incident Response Centre* (Centro Canadiense de Respuesta a Ciberincidentes); en Méjico están el UNAM-CERT, de la Universidad Nacional Autónoma de Méjico, y el CERT-MX; en Colombia, entre otros, se encuentran el colCERT (del Ministerio de Defensa), el CSIRTPONAL (de la Policía Nacional) y el SOC-CCOC (*Security Operations Center - Cyber Operations Command Joint*, Centro de Operaciones de Seguridad – Mando Conjunto de Ciberoperaciones) para las fuerzas

[79] La Unión Internacional de Telecomunicaciones utiliza las siglas CIRT en su programa de ayuda para implantar este tipo de centros por todo el mundo.

armadas y operadores de infraestructuras críticas; en Brasil, el CERT.br; en Chile el equipo CSIRT Chile y en Venezuela el VenCERT.

Los países de Asia y Oceanía disponen de multitud de equipos similares: se pueden mencionar el JPCERT/CC japonés, primer CSIRT del país, que actúa como un equipo de coordinación del resto de equipos de Japón, el CNCERT/CC de la República Popular de China, CERT-In de India, CERT Australia, HKCERT de Hong Kong, KrCERT/CC de Corea del Sur, MyCERT de Malasia, ThaiCERT de Tailandia o VNCERT de Vietnam entre otros. Nueva Zelanda no tiene un CERT o CSIRT como tal, aunque las funciones equivalentes las realiza el *National Cyber Security Centre* (Centro Nacional de Ciberseguridad), creado a raíz de la estrategia nacional de ciberseguridad de 2011. En el mismo documento se indicaba la posibilidad de realizar un estudio futuro sobre la necesidad crear un CERT, aunque de momento no existe.

En ocasiones se crean organizaciones internacionales que agrupan a diversos CERT/CSIRT que deseen formar parte de ellas, con objeto de compartir metodologías y experiencias, además de organizar reuniones y foros diversos. Como ejemplo a nivel mundial, hay un foro llamado FIRST (*Forum of Incident Response and Security Teams*, Foro de Equipos de Seguridad y Respuesta a Incidentes)(251). A esta organización pertenecen 290 equipos de todo el mundo, incluyendo 10 españoles. Surgió en 1990, un año después de que se creara el primer CERT en la Universidad de Carnegie Mellon. En otras ocasiones, se agrupan CERT/CSIRT de diversas naciones dentro de un ámbito determinado; es el caso del APCERT (*Asia Pacific Computer Emergency Response Team*, Equipo de Respuesta a Emergencias Informáticas de Asia-Pacífico), organización que agrupa a los organismos correspondientes a 26 países de la zona oriental del mundo(252). En Europa existe el llamado *EGC Group*(253), una organización que agrupa CERT gubernamentales europeos. Pertenecen a este grupo 10 centros: CERT-Hungary (Hungría), CERTA (Francia), SITIC (Suecia), GOVCERT.NL (Holanda), CERT-Bund (Alemania), NorCERT (Noruega), CERT-FI (Finlandia), CSIRTUK y GovCertUK (Reino Unido) y el CCN-CERT español.

En cualquier caso, puede observarse una circunstancia digna de análisis: actualmente existen muchísimos centros de respuesta (CERT o CSIRT) en todo el mundo, incluso dentro de cada país suele haber varios. También hay multitud de organizaciones y unidades individuales dentro de los cuerpos policiales que se dedican a las mismas labores. Esta proliferación de centros de respuesta a incidentes y de cuerpos policiales puede ser un inconveniente en algunos casos, pues uno de los pilares en la lucha contra el cibercrimen es la información referente a incidentes ocurridos, técnicas utilizadas por los ciberdelincuentes, tendencias en cuanto a desarrollo de *malware*, comunicaciones entre delincuentes o bandas, análisis forenses, etc. Esta información se recopila por los distintos actores que intervienen en la prevención, investigación y persecución del cibercrimen, y es fundamental que haya un intercambio fluido y constante. Si no es así, no se puede aprovechar la experiencia de un centro para que beneficie al resto de centros de su entorno o de otros países. Evidentemente, a mayor número de

organismos implicados, mayor necesidad de coordinación existe para que la información fluya adecuadamente.

4.3 LEGISLACIÓN PENAL

Las estrategias y políticas concretas de cada ámbito en particular suelen indicar el camino a seguir y también algunas acciones concretas en forma de creación de organismos de lucha contra el cibercrimen y de respuesta y coordinación a nivel nacional e internacional. Sin embargo, de nada sirve establecer estrategias y políticas, crear equipos de coordinación y respuesta ante incidentes, y potenciar grupos de las fuerzas y cuerpos de seguridad para poder combatir el cibercrimen si posteriormente no existen instrumentos legales para que se pueda investigar adecuadamente y posteriormente entregar a los delincuentes a la justicia para que sean procesados y condenados. Existen multitud de aspectos que deben ser contemplados para que el paso final en la prevención y castigo del cibercrimen tenga éxito, y por eso para poder perseguir y castigar los ciberdelitos se hace necesario en muchos casos adaptar el ordenamiento jurídico en distintos ámbitos. En este sentido las distintas estrategias de ciberseguridad analizadas anteriormente suelen incluir este aspecto cuando no existe una adaptación previa de las disposiciones jurídicas en cuestión.

Hay diversas dificultades en el ordenamiento jurídico internacional tanto en el derecho procesal como en el derecho penal sustantivo[80]. Las cuestiones de competencia y jurisdicción son algunos de los principales problemas existentes. En todo el proceso de investigación y condena de los cibercriminales se hace necesario tomar una serie de acciones. Las fuerzas policiales que se hagan cargo de los casos deben poder realizar una investigación y una recogida de pruebas incriminatorias, para poner a disposición de la justicia a los cibercriminales y que éstos sean juzgados y condenados. En este proceso, la territorialidad ha sido tradicionalmente el fundamento para la atribución de competencias tanto a nivel nacional como internacional. Sin embargo, en el ciberespacio confluye una serie de circunstancias que impiden aplicar ese argumento en los procedimientos procesales. Ya se indicó en el punto 2.3 que el ciberespacio ofrece ventajas para la comisión de delitos; uno de ellos era la inexistencia de fronteras físicas, de tal manera que desde cualquier parte del mundo pueden cometerse actos ilícitos que afectan a ciudadanos de países muy distantes. Esta situación plantea dudas acerca de la jurisdicción competente para actuar en estos casos: ¿debería actuar la policía del país de donde es natural el ciberdelincuente, la del país desde donde se comete el ciberdelito o la del país de la víctima? Y si ha habido intermediarios en el proceso, como se vio en el punto 3.3 al hablar de las mulas, o incluso se ha utilizado como instrumentos de la

[80] El derecho penal sustantivo se refiere al conjunto de regulaciones legales que determinan qué delitos son punibles y qué penas les corresponden; el derecho penal procesal se refiere a los procedimientos para poder aplicar el derecho penal sustantivo, englobando asimismo aspectos como el derecho a la defensa de la parte acusada o la organización de los distintos tribunales de justicia.

comisión del delito a ordenadores pertenecientes a redes zombi situados en terceros países, ¿cómo se realizan las correspondientes acciones de investigación y judiciales? ¿Puede la policía de un país realizar investigaciones sobre equipos que se encuentran físicamente en otro país sin pedirle permiso a este último? Es más: en caso de que se demuestre que efectivamente ciudadanos residentes en otro país han realizado alguna acción delictiva, ¿admitiría este último las pruebas recogidas si no se han autorizado previamente? Y en caso de admitirlas, ¿cómo se puede proceder a su detención? Lo habitual es realizar órdenes de busca y captura, para lo cual se requieren acuerdos entre los países implicados que incluyan la posibilidad de extradición para que los delincuentes detenidos puedan ser trasladados a otro país para ser juzgados. Sin embargo, como se adelantó en el punto 2.3, no todos los países muestran actitudes de colaboración en casos de ciberdelitos. Los argumentos esgrimidos son variados, y en algunos casos ni siquiera se presentan argumentos, sino que simplemente se recurre a tácticas de falta de respuestas. Ejemplo de ello fue la falta de colaboración de las autoridades y proveedores de servicio de Rusia tras los ataques sufridos por Estonia en 2007.

La cuestión de la jurisdicción no es la única dificultad que se encuentra en la persecución del cibercrimen. La falta de adecuación de los distintos ordenamientos jurídicos ha sido otra traba que se ha encontrado durante años. Es necesario que los distintos países que quieran luchar contra la ciberdelincuencia se pongan de acuerdo con objeto de homogeneizar las disposiciones legales jurídicas que permitan la lucha contra los ciberdelincuentes. No es conveniente que los infractores se amparen en situaciones en las que una determinada acción sea delito en un país pero no en otro. Para ello es necesario en primer lugar que se realicen reformas jurídicas particulares que permitan una correcta tipificación de cada acto ilícito cometido. En las reformas penales que se hagan en ese sentido hay que tener en cuenta que las TIC pueden emplearse como instrumentos de comisión de delitos o bien como fin último de dichos delitos. Esto lleva a la discusión sobre si, para modificar los códigos penales antiguos, deben considerarse los ciberdelitos como figuras delictivas nuevas o bien si no suponen tipologías nuevas, sino meros medios y métodos alternativos. En cualquiera de los dos casos, es conveniente que se adapten las penas a las circunstancias específicas, pues no hacerlo puede suponer un refugio para los ciberdelincuentes, que verían que las penas impuestas son de una entidad pequeña en relación a las ganancias adquiridas, o incluso que los delitos cometidos no son castigados por vacío legal. En este sentido puede ayudar el hecho de que, en diversas estrategias de ciberseguridad (como la española, de reciente aprobación), se contemple que los ciberdelitos han pasado de ser simples actos ilícitos con fines lucrativos a una verdadera amenaza para la seguridad de las naciones.

En relación a la adaptación de las disposiciones legales penales, hay que destacar la aprobación en 2001 del Convenio sobre la Ciberdelincuencia (más conocido como Convenio de Budapest) el 23 de noviembre de 2001(63)(64). Ya se habían publicado algunas recomendaciones anteriormente, como la R(95)13(254), que hablaba sobre los problemas de los derechos penales sustantivos en relación con las tecnologías de la información, que a su vez venía a completar de alguna manera lo recomendado anteriormente en las publicaciones R(81)20(255), R(85)10 (256), R(87)15(257) y

R(89)9(258). Sin embargo, todas ellas abordaban de forma puntual y muy breve (la longitud del mayor de estos documentos es de 3 páginas) algunos aspectos individuales relacionados con las pruebas informáticas, interceptación de las comunicaciones o el uso de datos personales por parte de las fuerzas policiales. El Convenio de Budapest aunaba en un solo documento prácticamente todo lo que podía ser necesario legislar para empezar a regular la lucha contra el cibercrimen, por lo que su publicación supuso un hito histórico. Multitud de países de todo el mundo, no solo pertenecientes al Consejo de Europa, han firmado y ratificado el convenio, adaptando sus disposiciones nacionales de acuerdo con él; otros lo han firmado, aunque no lo han ratificado aún, y hay muchos que han manifestado en distintas estrategias de ciberseguridad analizadas su deseo de adherirse a él[81]. El documento pretende ser un instrumento útil de lucha contra el cibercrimen, mediante la adopción de políticas penales comunes yla mejora de la cooperación internacional y entre los estados y el sector privado, sin descuidar la protección de los derechos y libertades fundamentales. Para ello ofrece disposiciones de derecho penal sustantivo, tipificando detalladamente multitud de ciberdelitos, e incluyendo los supuestos de complicidad y tentativa. En lo que se refiere al derecho penal procesal, ofrece disposiciones acerca de la conservación de datos informáticos almacenados, registro y decomiso de dichos datos y recogida en tiempo real de los mismos, entre otras. Importante es la sección dedicada a las competencias, pues aunque es breve, permite establecer unos criterios básicos para los estados que se hayan adherido al convenio. El capítulo dedicado a la cooperación internacional establece principios generales al respecto, contemplando la extradición y la colaboración.

España publicó el Instrumento de Ratificación del Convenio de Budapest en 2010, entrando en vigor el 1 de octubre de ese año(259). En dicho Instrumento, publicado el 17 de septiembre de 2010 en el Boletín Oficial del Estado, se incluía una Declaración acerca de la eventual participación de Gibraltar en la aplicación del Convenio. Contando a nuestro país, en total han firmado el convenio 49 países (4 de los cuales no pertenecen al Consejo de Europa); de los que lo han firmado, 11 no lo han ratificado. El número total de países que han ratificado el Convenio es 41 (5 de ellos no son miembros del Consejo de Europa, y 3 no lo habían firmado previamente: Australia, República Dominicana y Mauricio).

El Convenio de Budapest no es el único texto de referencia internacional en lo que se refiere a recomendaciones de legislación, aunque sea el más conocido y apreciado. La UIT redactó en 2009 el llamado "*Toolkit for Cybercrime Legislation*"(260)(261), con la intención de ayudar a implementar disposiciones legales mediante una terminología legislativa común y multitud de referencias. La terminología fue realizada tras realizar un análisis general de la legislación de distintos países desarrollados y del Convenio sobre la Ciberdelincuencia, con el objetivo de servir de guía para el desarrollo o modificación de

[81] Puede consultarse la lista de países que lo han firmado y/o ratificado en http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

leyes particulares sobre el cibercrimen. El documento en su conjunto tenía como objetivo armonizarlas leyes sobre el cibercrimen en el entorno internacional, sirviendo como un recurso común tanto para legisladores como para políticos, estamentos gubernamentales, actores judiciales y representantes de la industria. En ese sentido realizaba una aproximación similar a la ofrecida por el Convenio de Budapest, proporcionando en primer lugar definiciones de términos que se utilizarían a lo largo del documento, para a continuación ofrecer una lista de delitos, agrupados en las siguientes categorías:

- Uso no autorizado de ordenadores, sistemas de ordenadores y redes
- Acceso no autorizado o adquisición de datos de ordenadores, de contenido o de tráfico
- Interferencia y trastorno
- Interceptación
- Mal uso y *malware*
- Falsificación digital
- Fraude digital, procurando beneficios económicos
- Extorsión
- Colaboración, encubrimiento y tentativa
- Responsabilidad corporativa

Dentro de cada categoría se indican en el documento distintos delitos, diferenciados en cuanto a si los actos ilícitos tienen como objetivos ordenadores gubernamentales, equipos relacionados con infraestructuras críticas u otros, incluyendo el propósito claro de terrorismo.

Otros documentos del mismo organismo estaban enfocados a un conjunto de 15 países pertenecientes a África, Caribe y zona del Pacífico, llamado ACP (*African, Caribbean and Pacific States*) en el entorno de la UIT. Entre ellos está el titulado "*Cybercrimes/e-Crimes: Model Policy Guidelines & Legislative Texts*"(262), dirigido en particular a la zona del Caribe, el cual menciona también algunos de los delitos que debían considerarse (acceso ilegal, estancia ilegal, interceptación ilegal, interferencia ilegal de datos, espionaje de datos, etc.). Otro documento del mismo grupo, dirigido a los países situados en las islas del Océano Pacífico, es el titulado "*Electronic Crimes: Knowledge-based Report*"(263), que menciona exactamente los mismos delitos que el anterior. Por otra parte, la UIT firmó en 2011 un acuerdo de entendimiento (*Memorandum of Understanding, MOU*) con UNODC (*United Nations Office on Drugs and Crime*, Oficina de las Naciones Unidas contra la Droga y el Delito) para proporcionar apoyo en forma de estudios de normativas, revisión de legislación y asistencia técnica a los países que lo necesiten(264).

Una vez se decide por parte de algún país la modificación de sus ordenamientos jurídicos para adaptarlos a las nuevas formas de delincuencia, la inclusión de las actividades ilícitas puede hacerse de dos maneras: proporcionando un tratamiento conjunto y diferenciado a los ciberdelitos, o bien adaptando los distintos artículos

concretos ya existentes, modificándolos para incluir el uso de las TIC como instrumento u objeto de los delitos previamente contemplados. En nuestro país se ha adoptado la segunda opción, por lo que no cabe esperar encontrar algún título, capítulo o sección exclusivos para los ciberdelitos. Es interesante notar que el código penal de 1995(265) ya contemplaba la utilización de las nuevas tecnologías en su articulado; así, y como ejemplo, el artículo 197 especificaba:

> *1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas,* ***mensajes de correo electrónico*** *o cualesquiera otros documentos (…)*
>
> *2.Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o* ***soportes informáticos, electrónicos o telemáticos****, o en cualquier otro tipo de archivo o registro público o privado.*

Posteriormente ha sido revisado en 27 ocasiones (la última publicada el 28 de diciembre de 2012, entrando en vigor el 17 de enero de 2013). Varias de las modificaciones han tenido relación precisamente con la temática de este Proyecto. El punto 3 del artículo antes referido era así en el texto original:

> *3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

y queda así en el texto consolidado actual:

> *3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*

En España ha habido otras iniciativas legislativas alrededor de la seguridad en las comunicaciones y con efectos en la lucha contra el cibercrimen. Como ejemplo de ello puede citarse la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, basada en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, que modifica a la anterior 2002/58/CE. La Ley menciona el uso con “fines indeseados, cuando no delictivos” de las redes de telefonía y de comunicaciones electrónicas en general, y obliga a los operadores de telecomunicaciones a retener ciertos datos que puedan ser requeridos

por agentes facultados (básicamente cuerpos policiales autorizados, Centro Nacional de Inteligencia y funcionarios de Vigilancia Aduanera en el desarrollo de sus funciones como policía judicial). También se creó, en 2010(266), la figura del Fiscal de Sala coordinador de la criminalidad informática, en línea con la anterior creación de semejantes puestos especializados en otras áreas de actuación (antidroga y contra la corrupción y la delincuencia organizada, contra la violencia sobre la mujer, seguridad vial, extranjería y otros). Se asignaron sus funciones en 2011(267), entre las que se encuentran la coordinación de los distintos fiscales que se ocupen de temas relacionados con la ciberdelincuencia y las relaciones con las diversas unidades policiales especializadas en la materia. Se establecen asimismo las áreas que serán competencia del nuevo fiscal, en tres categorías:

a) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC
b) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC
c) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia

De esta manera el Estado se asegura de que puede cumplir sus funciones encomendadas en el entorno del Ministerio Fiscal, además de colaborar con las fuerzas policiales para perseguir y esclarecer hechos delictivos de su competencia realizados en el ciberespacio.

Con todo lo que se ha visto en este capítulo, puede extraerse la conclusión de que hay una amplia cantidad de iniciativas a distintos niveles y en diversos entornos destinadas a intentar evitar las actividades ilegales y altamente peligrosas que se llevan a cabo en el ciberespacio. Se han establecido marcos legales en ámbitos nacionales e internacionales, hay grupos de lucha contra el cibercrimen y el ciberterrorismo y la legislación penal se va adaptando poco a poco a las nuevas circunstancias para conseguir una efectividad adecuada en el esfuerzo constante por combatir las actividades ilegales en el ciberespacio.

CONCLUSIONES

Tras el profundo análisis realizado, que abarca diferentes facetas del cibercrimen y del ciberterrorismo, queda claro que estos fenómenos constituyen una seria amenaza para la sociedad. Quizá puedan considerarse estas actividades como una extensión de las equivalentes en el mundo físico no virtual, pero evidentemente hay elementos que las diferencian y que exigen un esfuerzo adicional y un trabajo altamente especializado.

En el mundo desarrollado actual, tan dependiente de las nuevas tecnologías, cualquier ciudadano, empresa o administración es víctima potencial de multitud de acciones contra la seguridad. Los actos delictivos se llevan a cabo diariamente por todo el mundo, a pequeña y a gran escala. Son muchos y muy variados los actores que intervienen en el complejo mundo de la ciberdelincuencia y el ciberterrorismo. Las pérdidas económicas sufridas como consecuencia de estas actividades son enormes. Las herramientas y técnicas utilizadas para cometer actos delictivos van evolucionando y se van mejorando conforme pasa el tiempo y son descubiertas por los investigadores. Teniendo en cuenta estas circunstancias y otras analizadas con detalle en este trabajo y que juegan a favor de delincuentes y terroristas, puede entenderse que el esfuerzo para combatir los fenómenos objeto de estudio no es nada fácil. En esta labor es imprescindible contar con un marco legal adecuado que permita desarrollar labores destinadas a evitar la comisión de actos ilícitos, a minimizar su impacto en caso de que ocurran y a perseguir a sus autores. También serán de vital importancia los equipos que luchan contra las actividades ilegales, pero en este aspecto hay algo que debe tenerse en cuenta: la proliferación de organismos destinados a luchar contra el cibercrimen y el ciberterrorismo puede conllevar problemas de intercambio de información y de coordinación en las distintas acciones llevadas a cabo. Será imprescindible realizar una planificación adecuada de los recursos humanos y materiales puestos a disposición de las fuerzas policiales y las instancias judiciales, y llegado el caso, reorganizar las fuerzas existentes para mayor aprovechamiento y efectividad.

Queda mucho camino por recorrer en la lucha contra las actividades ilegales en el ciberespacio, y desde luego para tener éxito en esa pugna es imprescindible un conocimiento profundo del entorno y de todas las circunstancias que rodean al mundo de la delincuencia y el terrorismo en este ámbito. La incorporación de un número cada vez mayor de dispositivos a las redes globales de comunicación complica mucho las labores policiales y judiciales: los equipos móviles personales se han expandido y han alcanzado niveles de penetración en la sociedad inimaginables hace años, y en el futuro multitud de equipos electrónicos invadirán los hogares de millones de personas, facilitando la vida y proporcionando comodidad, pero también constituyendo una vía de entrada potencial a nuestro espacio privado. Estas nuevas circunstancias serán sin duda aprovechadas por los delincuentes, que intentarán conseguir beneficios de cualquier fallo de seguridad por pequeño que sea. Por lo tanto, todo parece indicar que en el

futuro estas amenazas aumentarán en extensión e intensidad. Será fundamental invertir en medios y educación para luchar contra un peligro que no ha hecho más que empezar y que nunca acabará.

REFERENCIAS

1. **Di Camillo, Federica y Miranda, Valérie.** [En línea] septiembre de 2011. [Citado el: 23 de noviembre de 2013.] Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward.

2. **RAE.** ciber. [En línea] 2013. [Citado el: 1 de diciembre de 2013.] http://lema.rae.es/drae/?val=ciber.

3. —. delito. [En línea] 2013. [Citado el: 1 de diciembre de 2013.] http://lema.rae.es/drae/?val=delito.

4. —. terrorismo. [En línea] 2013. [Citado el: 1 de diciembre de 2013.] http://lema.rae.es/drae/?val=terrorismo.

5. New Zealand's Cyber Security Strategy. [En línea] junio de 2011. [Citado el: 15 de noviembre de 2013.] http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf.

6. **McAfee.** Cybercrime Exposed - Cybercrime-as-a-Service. [En línea] 2013. [Citado el: 27 de enero de 2014.] http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf.

7. **Koetsier, John.** Massive Android flaw lets hackers 'take over' and 'control' 99% of Android devices (updated). [En línea] 3 de julio de 2013. [Citado el: 15 de noviembre de 2013.] http://venturebeat.com/2013/07/03/massive-android-flaw-allows-hackers-to-take-over-and-control-99-of-android-devices/.

8. **Naciones Unidas.** Corte Penal Internacional. [En línea] 17 de julio de 1998. [Citado el: 21 de noviembre de 2013.] http://www.un.org/spanish/law/icc/statute/final.htm. A/CONF.183/10*.

9. **Consejo de Europa.** [En línea] 27 de enero de 1977. [Citado el: 23 de noviembre de 2013.] http://conventions.coe.int/Treaty/en/Treaties/Html/090.htm.

10. —. [En línea] 16 de mayo de 2005. [Citado el: 23 de noviembre de 2013.] http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm.

11. Press Conference on the Results of the G8 Justice and Home Affairs Ministerial, Moscow, 16 June 2006. [En línea] 16 de junio de 2006. [Citado el: 23 de noviembre de 2013.] http://www.statewatch.org/news/2006/jul/02g8-jha-press-statement-jun-2006.htm.

12. **CCN.** Pronostican un ataque terrorista a gran escala en Internet. [En línea] 23 de febrero de 2007. [Citado el: 15 de noviembre de 2013.] https://www.ccn-

cert.cni.es/index.php?option=com_content&view=article&id=1500:pronostican-un-ataque-terrorista-a-gran-escala-en-internet&catid=61&Itemid=197&lang=es.

13. **Lewis, James A.** [En línea] diciembre de 2002. [Citado el: 23 de noviembre de 2013.] http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

14. **William L. Tafoya, Ph.D.** Cyber Terror. [En línea] noviembre de 2011. [Citado el: 23 de noviembre de 2013.] http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror.

15. **Collin, Barry.** [En línea] marzo de 1997. [Citado el: 23 de noviembre de 2013.] http://www.cjimagazine.com/archives/cji4c18.html?id=415.

16. **CNN.** [En línea] 1 de mayo de 2012. [Citado el: 24 de noviembre de 2013.] http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html.

17. **Shelly, Louise.** El financiamiento del terrorismo. [En línea] otoño de 2005. [Citado el: 24 de noviembre de 2013.] http://sartraccc.ru/Pub/shelle%2813-10-05%29.pdf.

18. **BBC.** As it happened: Mumbai attacks 27 Nov. [En línea] 27 de noviembre de 2008. [Citado el: 3 de enero de 2014.] http://news.bbc.co.uk/2/hi/south_asia/7752003.stm.

19. **Bumgarner, John.** Tech-savvy terrorists. [En línea] 1 de abril de 2011. [Citado el: 3 de enero de 2014.] http://apdforum.com/en_GB/article/rmiap/articles/print/features/2011/04/01/feature-01.

20. **UIT-T.** T-REC-X.1205-200804-I. [En línea] abril de 2008. [Citado el: 23 de noviembre de 2013.] http://www.itu.int/rec/T-REC-X.1205-200804-I.

21. —. Ciberseguridad. [En línea] 2012. [Citado el: 23 de noviembre de 2013.] http://www.itu.int/en/wcit-12/Documents/WCIT-background-brief6-S.pdf.

22. **The Washington Post.** China continues to deny carrying out cyberattacks against U.S. [En línea] 29 de mayo de 2013. [Citado el: 15 de noviembre de 2013.] http://www.washingtonpost.com/world/asia_pacific/china-continues-to-deny-us-cyber-attack-accusations/2013/05/29/a131780e-c85e-11e2-9245-773c0123c027_story.html.

23. **The Register.** US power grid the target of 'numerous and daily' cyber-attacks. [En línea] 23 de mayo de 2013. [Citado el: 15 de noviembre de 2013.] http://www.theregister.co.uk/2013/05/23/us_power_grid_cyber_attack_report/.

24. **U.S. News & World Report.** U.S. Nukes Face Up to 10 Million Cyber Attacks Daily. [En línea] 20 de marzo de 2012. [Citado el: 15 de noviembre de 2013.] http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

25. Cyber Attacks Statistics. [En línea] 19 de enero de 2014. [Citado el: 27 de enero de 2014.] http://hackmageddon.com/category/security/cyber-attacks-statistics/.

26. Cyberattack map shows U.S. continuously under assault. [En línea] 22 de octubre de 2013. [Citado el: 15 de enero de 2013.] http://dailycaller.com/2013/10/22/cyberattack-map-shows-u-s-continuously-under-assault/.

27. Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space. [En línea] junio de 2009. [Citado el: 15 de noviembre de 2013.] http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.

28. **Consejo de la Unión Europea.** [En línea] 8 de diciembre de 2008. [Citado el: 29 de noviembre de 2013.] Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF.

29. **The White House.** Presidential Policy Directive -- Critical Infrastructure Security and Resilience. [En línea] 12 de febrero de 2013. [Citado el: 4 de diciembre de 2013.] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

30. Un fallo en la red eléctrica alemana deja una hora sin luz a millones de personas en Europa. [En línea] 4 de noviembre de 2006. [Citado el: 1 de diciembre de 2013.] http://elpais.com/elpais/2006/11/04/actualidad/1162631823_850215.html.

31. **CNN.** Major power outage hits New York, other large cities. [En línea] 15 de agosto de 2003. [Citado el: 1 de diciembre de 2013.] http://edition.cnn.com/2003/US/08/14/power.outage/.

32. **Holguin, Jaime.** Biggest Blackout In U.S. History. [En línea] 15 de agosto de 2003. [Citado el: 1 de diciembre de 2013.] http://www.cbsnews.com/news/biggest-blackout-in-us-history/.

33. http://revuln.com. [En línea] [Citado el: 1 de diciembre de 2013.] http://revuln.com.

34. RevVuln SCADA 0-day vulnerabilities. [En línea] [Citado el: 1 de diciembre de 2013.] http://vimeo.com/53806381.

35. **Department of Homeland Security.** [En línea] 2009. [Citado el: 30 de noviembre de 2013.] https://www.dhs.gov/publication/2009-national-infrastructure-protection-plan-and-supporting-documents.

36. —. [En línea] 17 de diciembre de 2003. [Citado el: 30 de noviembre de 2013.] http://www.dhs.gov/homeland-security-presidential-directive-7.

37. Presidential Policy Directive -- Critical Infrastructure Security and Resilience. [En línea] 12 de febrero de 2013. [Citado el: 30 de noviembre de 2013.] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

38. **Department of Homeland Security.** [En línea] [Citado el: 30 de noviembre de 2013.] http://www.dhs.gov/critical-infrastructure-sectors.

39. BOE. [En línea] 29 de abril de 2011. [Citado el: 30 de noviembre de 2013.] http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf.

40. **S. L. Koh, Collin y Chew, Alvin.** Journal of Energy Security. [En línea] 27 de agosto de 2009. [Citado el: 1 de diciembre de 2013.] http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructure-protection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349.

41. **Roberts, Paul.** Oil giant Saudi Aramco back online after 30,000 workstations hit by malware. [En línea] 27 de agosto de 2012. [Citado el: 1 de diciembre de 2013.] http://nakedsecurity.sophos.com/2012/08/27/saudi-aramco-malware/.

42. **Perlroth, Nicole.** In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. [En línea] 23 de octubre de 2012. [Citado el: 1 de diciembre de 2013.] http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

43. **BBC.** BBC. *Computer virus hits second energy firm.* [En línea] 31 de agosto de 2012. [Citado el: 1 de diciembre de 2013.] http://www.bbc.co.uk/news/technology-19434920.

44. **CNET.** CNET. *Virus knocks out computers at Qatari gas firm RasGas.* [En línea] 30 de agosto de 2012. [Citado el: 1 de diciembre de 2013.] http://news.cnet.com/8301-1009_3-57503641-83/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/.

45. **Gorman, Siobhan y Smith, Rebecca.** Electricity Grid in U.S. Penetrated By Spies. [En línea] 8 de abril de 2009. [Citado el: 1 de diciembre de 2013.] http://online.wsj.com/news/articles/SB123914805204099085.

46. EURACTIV. [En línea] 20 de diciembre de 2012. [Citado el: 1 de diciembre de 2013.] http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541.

47. **Bake, Stewart.** In the Dark - Crucial Industries Confront Cyberattacks. [En línea] 2010. [Citado el: 1 de diciembre de 2013.] http://www.mcafee.com/uk/resources/reports/rp-critical-infrastructure-protection.pdf.

48. **Broad, William J., Markoff, John y Sanger, David E.** Israeli Test on Worm Called Crucial in Iran Nuclear Delay. [En línea] 15 de enero de 2011. [Citado el: 1 de diciembre de 2013.] http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0.

49. **Falliere, Nicolas.** Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. [En línea] 6 de agosto de 2010. [Citado el: 1 de diciembre de 2013.] http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

50. **Efe.** Irán reconoce un ataque informático masivo contra sus sistemas industriales. [En línea] 27 de septiembre de 2010. [Citado el: 1 de diciembre de 2013.] http://www.elmundo.es/accesible/elmundo/2010/09/27/navegante/1285571297.html.

51. **Fildes, Jonathan.** Stuxnet worm 'targeted high-value Iranian assets'. [En línea] 23 de septiembre de 2010. [Citado el: 1 de diciembre de 2013.] http://www.bbc.co.uk/news/technology-11388018.

52. **Beaumont, Claudine.** Stuxnet virus: worm 'could be aimed at high-profile Iranian targets'. [En línea] 23 de septiembre de 2010. [Citado el: 1 de diciembre de 2013.] http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html.

53. **Emergui, Sal.** Israel y EEUU crearon el virus que dañó el programa nuclear iraní. [En línea] 16 de enero de 2011. [Citado el: 1 de diciembre de 2013.] http://www.elmundo.es/elmundo/2011/01/16/internacional/1295180388.html.

54. **Beresford, Dillon.** The sauce of utter pwnage. *Waking up the sleeping dragon.* [En línea] 9 de enero de 2011. [Citado el: 1 de diciembre de 2013.] http://thesauceofutterpwnage.blogspot.com.es/2011/01/waking-up-sleeping-dragon.html.

55. **Rashid, Fahmida Y.** Stuxnet-Like Trojans Can Exploit Critical Flaw in Chinese Industrial Software - See more at: http://www.eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/#sthash.0pJN2Upr.dpuf. [En línea] 12 de enero de 2011. [Citado el: 1 de diciembre de 2013.] http://www.eweek.com/c/a/Security/StuxnetLike-Trojans-Can-Exploit-Critical-Flaw-in-Chinese-Industrial-Software-296674/.

56. **Abrams, Marshall y Weiss, Joe.** Malicious Control System Cyber Security Attack Case Study. *NIST.* [En línea] 23 de julio de 2008. [Citado el: 1 de diciembre de 2013.] http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

57. **Danchev, Dancho.** SCADA Security Incidents and Critical Infrastructure Insecurities. [En línea] 5 de octubre de 2006. [Citado el: 1 de diciembre de 2013.] http://ddanchev.blogspot.com.es/2006/10/scada-security-incidents-and-critical.html.

58. **Brookes, Julian.** Rolling Stones. [En línea] 7 de junio de 2011. [Citado el: 8 de diciembre de 2013.] http://www.rollingstone.com/politics/blogs/national-affairs/one-in-four-hackers-is-an-fbi-mole-20110607.

59. **Yin, Sara.** 7 Hackers Who Got Legit Jobs From Their Exploits. *pcmag.com.* [En línea] 28 de junio de 2011. [Citado el: 8 de diciembre de 2013.] http://www.pcmag.com/slideshow/story/266255/7-hackers-who-got-legit-jobs-from-their-exploits/3.

60. **Piller, Charles.** U.S.-China Battle of 'Hacktivism' Escalates. [En línea] 2 de mayo de 2011. [Citado el: 8 de diciembre de 2013.] http://articles.latimes.com/2001/may/02/business/fi-58219.

61. **Gorman, Siobhan, Cole, August y Dreazen, Yochi.** Computer Spies Breach Fighter-Jet Project. [En línea] 21 de abril de 2009. [Citado el: 8 de diciembre de 2013.] http://online.wsj.com/news/articles/SB124027491029837401.

62. **Mick, Jason.** Chinese Hackers Score F-35, Black Hawk Chopper, and PATRIOT Missile Data. [En línea] 28 de mayo de 2013. [Citado el: 8 de diciembre de 2013.] http://www.dailytech.com/Chinese+Hackers+Score+F35+Black+Hawk+Chopper+and+PATRIOT+Missile+Data/article31638.htm.

63. **Europa, Consejo de.** Convenio sobre la ciberdelincuencia. [En línea] 23 de noviembre de 2001. [Citado el: 8 de diciembre de 2013.] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF.

64. **Europe, Council of.** Convention on Cybercrime. [En línea] 23 de noviembre de 2001. [Citado el: 8 de diciembre de 2013.] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

65. **Sullivan, Bob.** Fake escrow site scam widens. [En línea] 17 de diciembre de 2002. [Citado el: 10 de diciembre de 2013.] http://www.nbcnews.com/id/3078510/#.UqYMOCc7zZ4.

66. Payment Services Directive. [En línea] 5 de diciembre de 2007. [Citado el: 10 de diciembre de 2013.] http://ec.europa.eu/internal_market/payments/framework/text/index_en.htm.

67. ebay España. *Usar servicios de depósito de garantía.* [En línea] [Citado el: 10 de diciembre de 2013.] http://pages.ebay.es/help/pay/escrow.html.

68. **Loterías y Apuestas del Estado.** Aviso sobre estafas por suplantación de identidad de Loterías y Apuestas del Estado. [En línea] [Citado el: 11 de diciembre de 2013.] http://www.loteriasyapuestas.es/es/aviso-sobre-estafas-por-suplantacion-de-identidad-de-loterias-y-apuestas-del-estado.

69. **Diario de Navarra.** Cuatro meses de prisión por hacer de intermediario en una estafa de internet. *diariodenavarra.es.* [En línea] 27 de octubre de 2011. [Citado el: 11 de diciembre de 2013.] http://www.diariodenavarra.es/noticias/navarra/mas_navarra/cuatro_meses_prision_por_hacer_intermediario_una_estafa_internet_47725_2061.html.

70. **Baquero, Antonio.** La mafia rusa utiliza españoles en paro como correos para las estafas ´on line´. [En línea] 17 de agosto de 2009. [Citado el: 13 de diciembre de 2013.] http://www.elperiodicomediterraneo.com/noticias/imprimir.php?id=484661.

71. PHISHING. Mulas y muleros. [En línea] 25 de marzo de 2013. [Citado el: 11 de diciembre de 2013.] http://tacticalegal.pro/blog/phishing-mulas-y-muleros/.

72. Twitter GDT Guardia Civil. [En línea] 9 de diciembre de 2013. [Citado el: 14 de diciembre de 2013.] https://twitter.com/GDTGuardiaCivil/status/409988786487971840.

73. **BBC.** Millions tricked by 'scareware' . [En línea] 19 de octubre de 2009. [Citado el: 10 de diciembre de 2013.] http://news.bbc.co.uk/2/hi/technology/8313678.stm.

74. —. Parking ticket leads to a virus . [En línea] 5 de febrero de 2009. [Citado el: 10 de diciembre de 2013.] http://news.bbc.co.uk/2/hi/technology/7872299.stm.

75. Una cadena de tiendas de EEUU sufre el robo de datos de 46 millones de tarjetas de crédito. [En línea] 30 de marzo de 2007. [Citado el: 13 de diciembre de 2013.] http://www.elmundo.es/navegante/2007/03/30/tecnologia/1175247092.html.

76. Robo masivo de datos en PlayStation Network. [En línea] 26 de abril de 2011. [Citado el: 13 de diciembre de 2013.] http://www.elotrolado.net/noticia_robo-masivo-de-datos-en-playstation-network-re-actualizado_19049.

77. **Madariaga, Bárbara.** El robo de datos a Adobe podría haber afectado a más de 150 millones de cuentas. [En línea] 11 de noviembre de 2013. [Citado el: 13 de diciembre de 2013.] http://www.csospain.es/El-robo-de-datos-a-Adobe-podria-haber-afectado-a-mas-de-150-/seccion-actualidad/noticia-134832.

78. **Symantec.** Internet Security Threat Report 2013. [En línea] abril de 2013. [Citado el: 13 de diciembre de 2013.] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

79. Identity Theft: Evolving with Technology. [En línea] abril de 2010. [Citado el: 10 de diciembre de 2013.] http://www.safercerritos.com/_pdfs/neighborhood_watch/2010/watch_report_apr_10.pdf.

80. **FBI.** Lawyers' Identities Being Used for Fake Websites and Solicitations. [En línea] [Citado el: 10 de diciembre de 2013.] http://www.fbi.gov/scams-safety/e-scams.

81. Google AdWords. [En línea] [Citado el: 13 de diciembre de 2013.] http://www.google.es/ads/adwords/how-it-works.html.

82. El 'fraude por click' le cuesta a Google mil millones de dólares al año. [En línea] 19 de septiembre de 2007. [Citado el: 13 de diciembre de 2013.] http://www.20minutos.es/noticia/278416/0/google/pierde/millones/.

83. **Panda Security.** Collaboration between Panda Software and RSA Security helps to dismantle the control system of a network for swindling 'pay per click' systems. [En línea] 12 de junio de 2006. [Citado el: 14 de diciembre de 2013.]

http://www.pandasecurity.com/belgium/homeusers/media/press-releases/viewnews?noticia=7461.

84. **Daswani, Neil, Stoppelman, Michael y Teams, Google Click Quality and Security.** The Anatomy of Clickbot.A. [En línea] [Citado el: 14 de diciembre de 2013.] https://www.usenix.org/legacy/events/hotbots07/tech/full_papers/daswani/daswani.pdf.

85. **Ramezany, Shahim.** Analyzing a Dom-Based XSS in Yahoo! [En línea] 2013. [Citado el: 14 de diciembre de 2013.] http://www.exploit-db.com/wp-content/themes/exploit/docs/24109.pdf.

86. **Protalinski, Emil.** Despite its efforts to fix vulnerabilities, Yahoo's Mail users continue reporting hacking incidents. [En línea] 6 de marzo de 2013. [Citado el: 14 de diciembre de 2013.] http://thenextweb.com/insider/2013/03/06/despite-its-efforts-to-fix-vulnerabilities-yahoos-mail-users-continue-reporting-hacking-incidents/#!pS0zm.

87. **Wheatley, Mike.** Yahoo Mail Hacked Again – Serious Questions Raised About Its Ability to Protect Users. [En línea] 30 de abril de 2013. [Citado el: 14 de diciembre de 2013.] http://siliconangle.com/blog/2013/04/30/yahoo-mail-hacked-again-serious-questions-raised-about-its-ability-to-protect-users/.

88. HP Training Center Official Website Hacked & Defaced. [En línea] 8 de diciembre de 2012. [Citado el: 14 de diciembre de 2013.] http://www.voiceofgreyhat.com/2012/08/HP-Training-Center-Official-Website-Hacked.html.

89. Secuestran dominios de Metasploit.com, Rapid7.com y empresas antivirus. [En línea] 14 de octubre de 2013. [Citado el: 14 de diciembre de 2013.] http://seguinfo.wordpress.com/category/defacing/.

90. Amanda Todd, caso dramático de sextorsión y ciberbullying analizado por PantallasAmigas. [En línea] 17 de octubre de 2012. [Citado el: 11 de enero de 2014.] http://www.ciberbullying.com/cyberbullying/2012/10/17/el-video-con-el-que-amanda-todd-luchaba-contra-el-ciberbullying-subtitulado-al-espanol-por-pantallasamigas/.

91. El GDT bloquea 690 páginas web dedicadas a la venta de productos falsificados. [En línea] 2 de diciembre de 2013. [Citado el: 14 de diciembre de 2013.] https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1232.

92. Op. TENGO - El GDT ha detenido un pedófilo por la distribución de más de 800.000 archivos . [En línea] 4 de diciembre de 2013. [Citado el: 14 de diciembre de 2013.] https://www.gdt.guardiacivil.es/webgdt/popup_noticia.php?id=1233.

93. antivirus.interbusca.com. [En línea] [Citado el: 15 de diciembre de 2013.] http://antivirus.interbusca.com/enciclopedia-virus/virus-w32_gruel-40323.html.

94. **ESET.** [En línea] [Citado el: 15 de diciembre de 2013.] http://www.eset-la.com/centro-amenazas/amenazas/Adware/2142.

95. **Moore, David, y otros.** Inside the Slammer worm. [En línea] 2003. [Citado el: 20 de diciembre de 2013.] http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf.

96. Chernobyl. [En línea] [Citado el: 9 de enero de 2014.] http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/encyclopedia/overview.aspx?idvirus=2860.

97. A 25 años de Chernobyl y a 12 años del (virus) Chernobyl. [En línea] 26 de abril de 2011. [Citado el: 9 de enero de 2014.] http://blogs.eset-la.com/laboratorio/2011/04/26/25-anos-chernobyl-12-anos-virus/.

98. Stealing Information and Exploitation: Form Grabbing. [En línea] [Citado el: 15 de diciembre de 2013.] http://www.infosectoday.com/Articles/Form_Grabbing/Form_Grabbing.htm.

99. **Panda Security.** Enciclopedia de Virus - Sinowal.CR. [En línea] [Citado el: 15 de diciembre de 2013.] http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/encyclopedia/overview.aspx?lst=det&idvirus=133983.

100. —. Enciclopedia de Virus - Rona.A. [En línea] [Citado el: 15 de diciembre de 2013.] http://www.pandasecurity.com/spain/homeusers/security-info/about-malware/encyclopedia/overview.aspx?lst=det&idvirus=76355.

101. **ESET.** Hesperbot – A New, Advanced Banking Trojan in the Wild. [En línea] 4 de septiembre de 2013. [Citado el: 20 de diciembre de 2013.] http://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/.

102. —. Hesperbot – Technical analysis part 1/2. [En línea] 6 de septiembre de 2013. [Citado el: 20 de diciembre de 2013.] http://www.welivesecurity.com/2013/09/06/hesperbot-technical-analysis-part-12/.

103. —. Hesperbot – technical analysis: part 2/2. [En línea] 9 de septiembre de 2013. [Citado el: 20 de diciembre de 2013.] http://www.welivesecurity.com/2013/09/09/hesperbot-technical-analysis-part-22/.

104. Cyber criminals using Android malware and ransomware the most. [En línea] 3 de junio de 2013. [Citado el: 15 de diciembre de 2013.] http://www.infoworld.com/t/security/mcafee-cyber-criminals-using-android-malware-and-ransomware-the-most-219916.

105. **Kaplan, Dan.** FBI ransomware scam finds new home on the Mac. [En línea] 16 de julio de 2013. [Citado el: 15 de diciembre de 2013.] http://www.scmagazine.com/fbi-ransomware-scam-finds-new-home-on-the-mac/article/303320/.

106. GDT - ¡Actividad Ilegal en su Sistema! . [En línea] 5 de agosto de 2011. [Citado el: 14 de diciembre de 2013.] https://www.gdt.guardiacivil.es/webgdt/alertas_gdt.php?id=180.

107. Das Bundeskriminalamt (BKA) warnt vor gefälschten E-Mails mit BKA-Absender - Enthaltene Links (URLs) auf keinen Fall öffnen! [En línea] 9 de diciembre de 2013. [Citado el: 14 de diciembre de 2013.] http://www.bka.de/DE/Presse/Pressemitteilungen/Presse2013/131209__GefaelschteBKAEMails.html?__nnn=true.

108. **Fraga, Brian.** Swansea police pay $750 "ransom" after computer virus strikes. [En línea] 15 de noviembre de 2013. [Citado el: 15 de diciembre de 2013.] http://www.heraldnews.com/news/x2132756948/Swansea-police-pay-750-ransom-after-computer-virus-strikes.

109. **Wagenseil, Paul.** Cryptolocker Ransomware Evolves to Spread on Its Own. [En línea] 3 de enero de 2014. [Citado el: 5 de enero de 2014.] http://www.tomsguide.com/us/cryptolocker-evolves-worm,news-18066.html.

110. **APWG.** Phishing Activity Trends Report – 2nd Quarter 2013. [En línea] 5 de noviembre de 2013. [Citado el: 18 de enero de 2014.] http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

111. —. Global Phishing Survey: Domain Name Use and Trends in 1H2013. [En línea] 18 de septiembre de 2013. [Citado el: 18 de enero de 2014.] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf.

112. **Der Spiegel.** Shopping for Spy Gear: Catalog Advertises NSA Toolbox. [En línea] 29 de diciembre de 2013. [Citado el: 18 de enero de 2014.] http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

113. **The Register.** Huawei dismisses NSA backdoor claims as profits soar. [En línea] 16 de enero de 2014. [Citado el: 18 de enero de 2014.] http://www.theregister.co.uk/2014/01/16/huawei_security_concerns_strong_financials/.

114. **TrendLabs.** Spyware Hides Behind Stolen Opera Digital Certificate. [En línea] 27 de junio de 2013. [Citado el: 11 de enero de 2014.]

115. —. FLAME Malware Heats Up The Threat Landscape. [En línea] 29 de mayo de 2012. [Citado el: 11 de enero de 2014.] http://blog.trendmicro.com/trendlabs-security-intelligence/flame-malware-heats-up-threat-landscape/.

116. —. Trend Micro Detects Reported Malicious Utilities with Adobe Certificates. [En línea] 3 de octubre de 2012. [Citado el: 11 de enero de 2014.] http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-detects-reported-malicious-utilities-with-adobe-certificates/.

117. Twitter DM spam/malware. [En línea] 30 de septiembre de 2013. [Citado el: 11 de enero de 2014.] http://isc.sans.edu/diary/Twitter+DM+spammalware/16688.

118. **McAfee.** McAfee Labs Threats Report: Third Quarter 2013. [En línea] 2013. [Citado el: 11 de enero de 2013.] http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf.

119. **Núñez, David García.** Estudio del troyano: Trojan-SMS-AndroidOS-FakePlayer.a. [En línea] agosto de 2010. [Citado el: 11 de enero de 2014.] http://www.hispasec.com/resources/troyano_android.pdf.

120. **Andrade, Marcos.** Golpe de Caixa Eletrônico Falso. [En línea] 8 de diciembre de 2013. [Citado el: 20 de enero de 2014.] https://www.youtube.com/watch?v=z1CrmlK5zMM.

121. **nakedsecurity.** Nordstrom finds cash register skimmers planted in Florida store. [En línea] 11 de octubre de 2013. [Citado el: 20 de enero de 2014.] http://nakedsecurity.sophos.com/2013/10/11/nordstrom-finds-cash-register-skimmers-planted-in-florida-store/.

122. **keydemon.com.** KeyGrabber Wi-Fi Premium. [En línea] [Citado el: 20 de enero de 2014.] http://www.keydemon.com/hardware_keylogger_wifi/.

123. **BBC Radio 4.** Cash machines raided with infected USB sticks. [En línea] 30 de diciembre de 2013. [Citado el: 20 de enero de 2014.] http://www.bbc.co.uk/news/technology-25550512.

124. **Díaz, Vicente.** Exploit de IE7 aprovechado para infección masiva . [En línea] 17 de diciembre de 2008. [Citado el: 16 de diciembre de 2013.] http://blog.s21sec.com/2008/12/exploit-de-ie7-aprovechado-para.html.

125. **Krebs, Brian.** Hacked Ad Seen on MySpace Served Spyware to a Million. [En línea] 20 de julio de 2006. [Citado el: 16 de diciembre de 2013.] http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html.

126. **Ferguson, Rik.** New York Times pushes Fake AV malvertisement. [En línea] 14 de septiembre de 2009. [Citado el: 16 de diciembre de 2013.] http://countermeasures.trendmicro.eu/new-york-times-pushes-fake-av-malvertisement/.

127. **Johnson, Bobbie.** Internet companies face up to 'malvertising' threat. [En línea] 25 de septiembre de 2009. [Citado el: 16 de diciembre de 2013.] http://www.theguardian.com/technology/2009/sep/25/malvertising.

128. **FBI.** New E-Scams & Warnings. [En línea] [Citado el: 9 de enero de 2014.] http://www.fbi.gov/scams-safety/e-scams.

129. Source Code for Zeus Crimeware Toolkit Disclosed. [En línea] 11 de mayo de 2011. [Citado el: 23 de diciembre de 2013.] http://www.infosecisland.com/blogview/13697-Source-Code-for-Zeus-Crimeware-Toolkit-Disclosed.html.

130. **Keizer, Gregg.** 'Gameover' malware is next-gen Zeus trojan. [En línea] 24 de enero de 2012. [Citado el: 23 de diciembre de 2013.] http://news.techworld.com/security/3332131/gameover-malware-is--next-gen-zeus-trojan/.

131. **paganinip.** Self-propagating ZeuS source code offered for sale in the underground. [En línea] 30 de junio de 2013. [Citado el: 23 de diciembre de 2013.] http://securityaffairs.co/wordpress/15728/cyber-crime/self-propagating-zeus-variant-underground.html.

132. **Walker, Danielle.** Zeus-family trojan spreads by way of spam botnet . [En línea] 5 de diciembre de 2012. [Citado el: 23 de diciembre de 2013.] http://www.scmagazine.com/zeus-family-trojan-spreads-by-way-of-spam-botnet/article/271333/.

133. **Leopando, Jonathan.** Blackhole Arrests - How Has The Underground Reacted? [En línea] 21 de octubre de 2013. [Citado el: 9 de enero de 2014.] http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-arrests-how-has-the-underground-reacted/.

134. **Dunn, John E.** Blackhole Exploit Kit in retreat as criminals defect to rival exploit system. [En línea] 23 de octubre de 2013. [Citado el: 9 de enero de 2014.] http://news.techworld.com/security/3475196/blackhole-exploit-kit-in-retreat-as-criminals-defect-to-rival-exploit-system/.

135. Cutwail Cybercriminals Replace BlackHole with Magnitude Exploit Kit. [En línea] 23 de octubre de 2013. [Citado el: 9 de enero de 2014.] http://csinfotechblog.wordpress.com/2013/10/23/cutwail-cybercriminals-replace-blackhole-with-magnitude-exploit-kit/.

136. Cutwail Spam Swapping Blackhole for Magnitude Exploit Kit. [En línea] 18 de octubre de 2013. [Citado el: 9 de enero de 2014.] http://www.secureworks.com/resources/blog/research/cutwail-spam-swapping-blackhole-for-magnitude-exploit-kit/.

137. **Symantec.** Android.Bmaster: A Million-Dollar Mobile Botnet. [En línea] 8 de febrero de 2012. [Citado el: 11 de enero de 2014.] http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet.

138. —. Android.Bmaster. [En línea] 8 de febrero de 2012. [Citado el: 11 de enero de 2014.] http://www.symantec.com/security_response/writeup.jsp?docid=2012-020609-3003-99.

139. Proofpoint - Defending the Ever-changing Now. [En línea] [Citado el: 25 de enero de 2014.] http://www.proofpoint.com/about-us/index.php.

140. **Proofpoint.** Proofpoint Uncovers Internet of Things (IoT) Cyberattack. [En línea] 16 de enero de 2014. [Citado el: 25 de enero de 2014.] http://www.proofpoint.com/about-us/press-releases/01162014.php.

141. —. Your Fridge is Full of SPAM: Proof of An IoT-driven Attack. [En línea] 16 de enero de 2014. [Citado el: 25 de enero de 2014.] http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-proof-of-a-Iot-driven-attack.php.

142. —. Your Fridge is Full of SPAM, part II: Details. [En línea] 21 de enero de 2014. [Citado el: 25 de enero de 2014.] http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-ll-details.php.

143. **cole, Eric.** *Advanced Persistent Threat. Understanding the danger and how to protect your organization.* s.l. : Elsevier, 2013. 978-1-59749-949-1.

144. **Higgins, Kelly Jackson.** APT Attackers Hit Japan's Biggest Defense Contractor . [En línea] 19 de septiembre de 2011. [Citado el: 20 de diciembre de 2013.] http://www.darkreading.com/attacks-breaches/apt-attackers-hit-japans-biggest-defense/231601696.

145. **Shakarian, Paulo, Shakarian, Jana y Ruef, Andrew.** *Introduction to cyber-warfare. A multidisciplinary approach.* s.l. : Elsevier, 2013. ISBN: 978-0-12407-814-7.

146. **Markoff, John.** Vast Spy System Loots Computers in 103 Countries . *The New York Times.* [En línea] 28 de marzo de 2009. [Citado el: 20 de diciembre de 2013.] http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=2&pagewanted=1&.

147. Freenet - The free network. [En línea] [Citado el: 19 de enero de 2014.] https://freenetproject.org.

148. I2P - El proyecto de internet invisible. [En línea] [Citado el: 19 de enero de 2014.] https://geti2p.net/es/.

149. TOR Project. [En línea] [Citado el: 19 de enero de 2014.] https://www.torproject.org/.

150. Onion Routing. [En línea] [Citado el: 19 de enero de 2014.] http://www.onion-router.net/.

151. US Naval Research Laboratory. [En línea] [Citado el: 19 de enero de 2014.] https://www.nrl.navy.mil/.

152. MorphMix. [En línea] [Citado el: 19 de enero de 2014.] https://home.zhaw.ch/~rer/projects/morphmix/.

153. Java Anonymity & Privacy. [En línea] [Citado el: 19 de enero de 2014.] http://anon.inf.tu-dresden.de/index_en.html.

154. Mixminion: A Type III Anonymous Remailer. [En línea] [Citado el: 19 de enero de 2014.] http://mixminion.net/.

155. ANts P2P. [En línea] [Citado el: 19 de enero de 2014.] http://antsp2p.sourceforge.net/.

156. MUTE - Simple, Anonymous File Sharing. [En línea] [Citado el: 19 de enero de 2014.] http://mute-net.sourceforge.net/.

157. **Schwartz, Mathew J.** FBI Admits To Tor Server Takeover. [En línea] 16 de septiembre de 2013. [Citado el: 1 de marzo de 2014.] http://www.informationweek.com/security/risk-management/fbi-admits-to-tor-server-takeover/d/d-id/1111553?.

158. **CNN.** FBI shuts down online drug market Silk Road. [En línea] 2 de octubre de 2013. [Citado el: 1 de marzo de 2014.] http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/.

159. **The Hacker News.** Firefox Zero-Day Exploit used by FBI to shutdown Child porn on Tor Network hosting; Tor Mail Compromised. [En línea] 4 de agosto de 2013. [Citado el: 1 de marzo de 2014.] http://thehackernews.com/2013/08/Firefox-Exploit-Tor-Network-child-pornography-Freedom-Hosting.html.

160. Canadá tiene el primer cajero automático para bitcoins. [En línea] 30 de octubre de 2013. [Citado el: 15 de enero de 2014.] http://www.infobae.com/2013/10/30/1520172-canada-tiene-el-primer-cajero-automatico-bitcoins.

161. Bitcoin's First ATM. [En línea] [Citado el: 15 de enero de 2014.]

162. **La Moncloa.** Golpe policial a una de las mayores redes cibercriminales especializada en infectar millones de ordenadores de todo el mundo. [En línea] 13 de febrero de 2013. [Citado el: 19 de enero de 2014.] http://www.lamoncloa.gob.es/ServiciosdePrensa/NotasPrensa/MIR/2013/130213policiainformatica.htm.

163. **el Periódico.** Desarticulada la banda que creó el virus informático "de la Policía". [En línea] 27 de septiembre de 2013. [Citado el: 19 de enero de 2014.] http://www.elperiodico.com/es/noticias/sociedad/desarticulada-banda-que-creo-virus-informatico-policia-2695652.

164. **Foster, Peter.** 'Bogus' AP tweet about explosion at the White House wipes billions off US markets. *The Telegraph.* [En línea] 23 de abril de 2013. [Citado el: 21 de diciembre de 2013.] http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

165. **McCarthy, Tom.** Syrian Electronic Army takes credit for attack on Obama's Twitter account. [En línea] 28 de octubre de 2013. [Citado el: 22 de diciembre de 2013.] http://www.theguardian.com/technology/2013/oct/28/barack-obama-twitter-hacked-syria.

166. **Ovide, Shira.** Skype Social Media Accounts Hacked by Syrian Electronic Army. [En línea] 1 de enero de 2014. [Citado el: 10 de enero de 2014.] http://blogs.wsj.com/digits/2014/01/01/skype-social-media-accounts-hacked-by-sea/.

167. **Gilbert, David.** WhatsApp, AVG and Alexa Hacked by Pro-Palestinian Kdms Team Hackers. [En línea] 8 de octubre de 2013. [Citado el: 21 de diciembre de 2013.] http://www.ibtimes.co.uk/kdms-team-pro-palistinian-hackers-whatsapp-avg-512269.

168. **Elbarakah, Tarik.** Moroccan hacking groups launch a massive cyber attack on Spain. [En línea] 21 de abril de 2013. [Citado el: 21 de diciembre de 2013.] http://www.moroccoworldnews.com/2013/04/87931/moroccan-hacking-groups-launch-a-massive-cyber-attack-on-spain/.

169. Op2M-Operation 2M-moroccan hackers-anonymous message to-30/06/2013. [En línea] 24 de mayo de 2013. [Citado el: 10 de enero de 2014.] http://www.youtube.com/watch?v=GU50XwbJfhU.

170. **Vamosi, Robert.** Botconomics, part II. [En línea] 6 de julio de 2007. [Citado el: 21 de diciembre de 2013.] http://reviews.cnet.com/4520-3513_7-6749973-1.html.

171. Anonymous Ecuador inició ataques a páginas gubernamentales del país y también de opositores. [En línea] 10 de agosto de 2012. [Citado el: 10 de enero de 2014.] http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=179151&umt=anonymous_ecuador_inicif3_ataques_a_pe1ginas_gubernamentales_del_paeds.

172. Anonymous anuncia ataque contra Chile el próximo lunes 22 de abril. [En línea] 16 de abril de 2013. [Citado el: 10 de enero de 2014.] http://www.latercera.com/noticia/tendencias/2013/04/659-519038-9-anonymous-anuncia-ataque-contra-chile-el-proximo-lunes-22-de-abril.shtml.

173. **EFE.** Anonymous amenaza con atacar a Japón si no detienen caza de delfines . [En línea] 11 de noviembre de 2013. [Citado el: 10 de enero de 2014.] http://www.primerahora.com/noticias/mundo/nota/anonymousamenazaconatacarajaponsinodetienencazadedelfines-970349/.

174. Anonymous ataca a Irán: roba 10 mil correos del gobierno y los lanza en un torrent en The Pirate Bay. [En línea] 3 de junio de 2011. [Citado el: 21 de diciembre de 2013.] http://alt1040.com/2011/06/anonymous-ataca-a-iran-roba-10-000-correos-del-gobierno-y-los-lanza-en-un-torrent-en-the-pirate-bay.

175. Anonymous ataca a los gobiernos de Egipto, Bahrein, Marruecos y Jordania y cuelga las claves de cientos de correos. [En línea] 6 de junio de 2011. [Citado el: 21 de diciembre de 2013.] http://alt1040.com/2011/06/anonymous-revela-las-contrasenas-de-los-correos-de-cientos-de-funcionarios-de-egipto-bahrein-marruecos-y-jordania.

176. **Lara, Rubén.** Ciberguerra de Anonymous contra el gobierno sirio a causa del apagón total de internet en el país . [En línea] 30 de noviembre de 2012. [Citado el: 21

de diciembre de 2013.] http://www.laproximaguerra.com/2012/11/ciberguerra-anonymous-siria-apagon-internet.html#.

177. **Greenwood, Phoebe.** Hackers leak Assad's astonishing office emails . [En línea] 7 de febrero de 2012. [Citado el: 21 de diciembre de 2013.] http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9067118/Anonymous-hackers-leak-Syrias-Bashar-al-Assads-astonishing-office-emails-discussing-Barbara-Walters.html.

178. Anonymous ataca más de 650 sitios web israelíes. [En línea] 19 de noviembre de 2012. [Citado el: 21 de diciembre de 2013.] http://www.pcactual.com/articulo/actualidad/noticias/11977/anonymous_ataca_mas_650_sitios_web_israelies.html.

179. **González, Daniel.** La Policía desarticula la "cúpula" de Anonymous en España. [En línea] 10 de junio de 2011. [Citado el: 21 de diciembre de 2013.] http://www.20minutos.es/noticia/1078201/0/policia/cupula/anonymous/.

180. 'Anonymous' ataca la web de la Policía Nacional en respuesta a las detenciones del viernes. [En línea] 12 de junio de 2011. [Citado el: 21 de diciembre de 2013.] http://www.20minutos.es/noticia/1080062/0/anonymous/policia/nacional/.

181. Anonymous publicará archivos que desvelan la corrupción del Gobierno español. [En línea] 25 de agosto de 2013. [Citado el: 21 de diciembre de 2013.] http://actualidad.rt.com/actualidad/view/103885-anonymous-operacion-espana-opsecretfiles2-corrupcion.

182. Anonymous publicará archivos que desvelan la corrupción del Gobierno español. [En línea] 25 de agosto de 2013. [Citado el: 21 de diciembre de 2013.] http://tercerainformacion.es/spip.php?article56816.

183. **Anderson, Nate.** How one man tracked down Anonymous—and paid a heavy price. [En línea] 10 de febrero de 2011. [Citado el: 22 de diciembre de 2013.] http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/.

184. **Bright, Peter.** Anonymous speaks: the inside story of the HBGary hack. [En línea] 16 de febrero de 2011. [Citado el: 22 de diciembre de 2013.] http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/.

185. Comienza la operación AntiSec: Lulzsec ataca al gobierno de Brasil y Anonymous envía un mensaje. [En línea] 22 de junio de 2011. [Citado el: 22 de diciembre de 2013.] http://alt1040.com/2011/06/comienza-la-operacion-antisec-lulzsec-ataca-al-gobierno-de-brasil-y-anonymous-envia-un-mensaje.

186. **Verza, María.** ¿Cómo funcionan Los Zetas? [En línea] 16 de julio de 2013. [Citado el: 10 de enero de 2014.] http://www.elmundo.es/america/2013/07/16/mexico/1373982845.html.

187. **Homeland Security News Wire.** Los Zetas decapitate blogger. [En línea] 14 de noviembre de 2011. [Citado el: 10 de enero de 2014.] http://www.homelandsecuritynewswire.com/los-zetas-decapitate-blogger.

188. **Kan, Paul Rexton.** Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico. [En línea] 26 de febrero de 2013. [Citado el: 10 de enero de 2014.]

189. **Mandiant.** APT1: Exposing One of China's Cyber Espionage Units. [En línea] 2013. [Citado el: 22 de diciembre de 2013.] http://intelreport.mandiant.com/.

190. **Higgins, Kelly Jackson.** Chinese Military Tied To Major Cyberespionage Operation . [En línea] 19 de febrero de 2013. [Citado el: 22 de diciembre de 2013.] http://www.darkreading.com/attacks-breaches/chinese-military-tied-to-major-cyberespi/240148807.

191. Russian Business Network (RBN) Exploit. [En línea] [Citado el: 21 de diciembre de 2013.] http://rbnexploit.blogspot.com.es/.

192. **The Shadowserver Foundation.** AS40989. RBN AS RBusiness Network. Clarifying the "guesswork" of Criminal Activity. [En línea] enero de 2008. [Citado el: 21 de diciembre de 2013.] http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf.

193. **Bizeul, David.** Russian Business Network study. [En línea] 20 de noviembre de 2007. [Citado el: 21 de diciembre de 2013.] http://www.bizeul.org/files/RBN_study.pdf.

194. **Hayton.** Russian Business Network malware sites and IP addresses. *McAfee.* [En línea] 29 de noviembre de 2011. [Citado el: 21 de diciembre de 2013.] https://community.mcafee.com/community/security/gti/webthreats/blog/2011/11/29/russian-business-network-malware-sites-and-ip-addresses.

195. **Greenwood, Chris.** 'Mr Big' of UK cyber-crime among gang of eight arrested over £1.3million Barclays computer hijack plot in carbon copy of Santander scam. [En línea] 20 de septiembre de 2013. [Citado el: 22 de diciembre de 2013.] http://www.dailymail.co.uk/news/article-2426519/Gang-arrested-1-3million-Barclays-hijack-plot-carbon-copy-Santander-scam.html.

196. Barclays Bank computer theft: Eight held over £1.3m haul. [En línea] 20 de septiembre de 2013. [Citado el: 22 de diciembre de 2013.] http://www.bbc.co.uk/news/uk-england-24172305.

197. **ABC Paraguay.** Ciberdelincuencia: Es más lucrativa que el narcotráfico". [En línea] 14 de enero de 2006. [Citado el: 23 de diciembre de 2013.] http://www.abc.com.py/edicion-impresa/suplementos/mundo-digital/ciberdelincuencia-es-mas-lucrativa-que-el-narcotrafico-880352.html.

198. **Cybersource.** Fraudsters Will Take $2.8 Billion out of eCommerce in 2005. [En línea] 2005. [Citado el: 23 de diciembre de 2013.] http://www.cybersource.com/news_and_events/view.php?page_id=1425.

199. **BBC.** Cyber criminals 'should get tough sentences' say police. [En línea] 10 de noviembre de 2011. [Citado el: 23 de diciembre de 2013.] http://www.bbc.co.uk/news/uk-15680466.

200. **Kovacs, Eduard.** ZeuS Trojan Bank Robbers Finally Convicted. [En línea] 5 de octubre de 2011. [Citado el: 23 de diciembre de 2013.] http://news.softpedia.com/news/ZeuS-Trojan-Bank-Robbers-Finally-Convicted-225533.shtml.

201. grc.com. [En línea] 21 de enero de 2014. [Citado el: 22 de enero de 2014.] https://www.grc.com/sn/sn-439-notes.pdf.

202. **Blue, Violet.** CryptoLocker's crimewave: A trail of millions in laundered Bitcoin. [En línea] 22 de diciembre de 2013. [Citado el: 22 de enero de 2014.] http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/.

203. **Dell SecureWorks.** CryptoLocker Ransomware. [En línea] 18 de diciembre de 2013. [Citado el: 22 de enero de 2014.] http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/.

204. **ZDNet.** Conficker's estimated economic cost? $9.1 billion. [En línea] 23 de abril de 2009. [Citado el: 25 de enero de 2014.] http://www.zdnet.com/blog/security/confickers-estimated-economic-cost-9-1-billion/3207.

205. **Ponemon Institute.** 2013 Cost of Cyber Crime Study: United States. [En línea] octubre de 2013. [Citado el: 10 de enero de 2014.] http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

206. —. The Impact of Cybercrime on Business. [En línea] mayo de 2012. [Citado el: 10 de enero de 2014.] http://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf.

207. **Greenberg, Andy.** Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. [En línea] 23 de marzo de 2012. [Citado el: 3 de enero de 2014.] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

208. **Microsoft.** Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet . [En línea] 5 de diciembre de 2013. [Citado el: 24 de diciembre de 2013.] http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx.

209. **Nadji, Yacin y Antonakakis, Manos.** Microsoft DCU — Strike Three. Now What? [En línea] diciembre de 2013. [Citado el: 24 de diciembre de 2013.] https://blog.damballa.com/archives/2221.

210. **BASCAP.** Estimating the global economic and social impacts of counterfeiting and piracy. [En línea] febrero de 2011. [Citado el: 13 de enero de 2014.] http://www.iccwbo.org/uploadedImages/Advocacy,_codes_and_rules/BASCAP/Library/Estimating%20the%20Global%20and%20Economic%20Impacts_Capture_source.PNG?n=425.

211. Observatorio de piratería y hábitos de consumo de contenidos digitales - segundo semestre de 2010. [En línea] abril de 2011. [Citado el: 13 de enero de 2013.] http://www.cedro.org/docs/textos-de-inter%C3%A9s/resumen_ejecutivo_estudio_pirateria_tercera_oleada.pdf?Status=Master.

212. Observatorio de piratería y hábitos de consumo de contenidos digitales 2012. [En línea] febrero de 2013. [Citado el: 13 de enero de 2014.] http://www.mcu.es/libro/img/MC/Observatorio_Pirateria_2012.pdf.

213. **Ruiter, Johan.** Cost of Cyber Crime largely met by businesses. [En línea] 10 de abril de 2012. [Citado el: 24 de diciembre de 2013.] https://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2012-04-10%2011:37:10.0&Taal=2.

214. Creado el Departamento de Seguridad Nacional dentro del Gabinete del Presidente del Gobierno. [En línea] 23 de julio de 2012. [Citado el: 13 de enero de 2014.] http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mpr/2012/230712_seguridadnacional.htm.

215. Estrategia de seguridad cibernética (Resolución) AG/RES. 2004. [En línea] 8 de junio de 2004. [Citado el: 15 de enero de 2014.] http://www.oas.org/es/ssm/cyber/documents/Estrategia-seguridad-cibernetica-resolucion.pdf.

216. The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world. [En línea] noviembre de 2011. [Citado el: 15 de enero de 2014.] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

217. **Rituerto, Ricardo Martínez de.** Los 'ciberataques' a Estonia desde Rusia desatan la alarma en la OTAN y la UE. [En línea] 18 de mayo de 2007. [Citado el: 1 de enero de 2014.] http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html.

218. Estonia protegerá sus instituciones de ataques informáticos con ayuda de la OTAN. [En línea] 18 de mayo de 2007. [Citado el: 1 de enero de 2014.] http://www.elmundo.es/navegante/2007/05/18/tecnologia/1179478759.html.

219. Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise. [En línea] noviembre de 2011. [Citado el: 1 de enero de 2014.] http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

220. Trustworthy cyberspace: strategic plan for the federal cybersecurity research and development program. [En línea] diciembre de 2011. [Citado el: 1 de enero de 2014.] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

221. Privacy Impact Assessment for the National Cybersecurity Protection System. [En línea] 30 de julio de 2012. [Citado el: 1 de enero de 2014.] http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

222. Common Security and Defence Policy. [En línea] 7 de mayo de 2010. [Citado el: 31 de diciembre de 2013.] http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0026_en.htm.

223. ENISA. [En línea] [Citado el: 15 de enero de 2014.] http://www.enisa.europa.eu/.

224. Europol. [En línea] [Citado el: 4 de enero de 2014.] https://www.europol.europa.eu/.

225. European Cybercrime Centre. [En línea] [Citado el: 4 de enero de 2014.] https://www.europol.europa.eu/ec3.

226. Centro Cibernético Policial - Policía Nacional de Colombia. [En línea] [Citado el: 15 de enero de 2014.] http://www.ccp.gov.co/.

227. Internet Crime. [En línea] [Citado el: 4 de enero de 2014.] http://www.bka.de/nn_194550/EN/SubjectsAZ/InternetCrime/internetCrime__node.html?__nnn=true.

228. Central Unit for Random Internet Searches (ZaRD). [En línea] [Citado el: 4 de enero de 2014.] http://www.bka.de/nn_195784/EN/SubjectsAZ/InternetCrime/ZaRD/internetCrimeZaRD__node.html?__nnn=true.

229. Cyber Crime Police Station. [En línea] [Citado el: 4 de enero de 2014.] http://www.hyderabadpolice.gov.in/frauds/cybercrimes.htm.

230. Cyber Crime Investigation Cell of Mumbai Police. [En línea] [Citado el: 4 de enero de 2014.] http://cybercellmumbai.gov.in/.

231. Keeping the UK safe in cyber space. [En línea] 12 de diciembre de 2013. [Citado el: 4 de enero de 2014.] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit.

232. **Brewster, Tom.** The Rush To Fix Britain's Cyber Police. [En línea] 20 de febrero de 2013. [Citado el: 4 de enero de 2014.] http://www.techweekeurope.co.uk/news/fixing-cyber-police-security-pceu-soca-national-crime-agency-106466.

233. National Cybersecurity & Communications Integration Center (NCCIC). [En línea] [Citado el: 4 de enero de 2014.] http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

234. **FBI.** responding-to-the-cyber-threat. [En línea] [Citado el: 4 de enero de 2014.] http://www.fbi.gov/news/testimony/responding-to-the-cyber-threat.

235. FBI Cyber Action Teams - Traveling the World to Catch Cyber Criminals. [En línea] [Citado el: 4 de enero de 2014.] http://www.fbi.gov/news/stories/2006/march/cats030606.

236. Internet Crime Complaint Center. [En línea] [Citado el: 4 de enero de 2014.] http://www.ic3.gov.

237. Electronic Crimes Task Forces and Working Groups. [En línea] [Citado el: 4 de enero de 2014.] http://www.secretservice.gov/ectf.shtml.

238. The Cell Phone Forensic Facility at the University of Tulsa. [En línea] [Citado el: 4 de enero de 2014.] The Cell Phone Forensic Facility at the University of Tulsa.

239. Grupo de Delitos Telemáticos - Unidad Central Operativa. [En línea] [Citado el: 10 de enero de 2014.] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php.

240. Grupo de Delitos Telemáticos - Twitter. [En línea] [Citado el: 10 de enero de 2014.] https://twitter.com/GDTGuardiaCivil.

241. Grupo de Delitos Telemáticos - Facebook. [En línea] [Citado el: 10 de enero de 2014.] https://es-es.facebook.com/GrupoDelitosTelematicos.

242. Grupo de Delitos Telemáticos - Tuenti. [En línea] [Citado el: 10 de enero de 2014.] http://www.tuenti.com/grupodelitostelematicos.

243. Grupo de Delitos Telemáticos - YouTube. [En línea] [Citado el: 10 de enero de 2014.] http://www.youtube.com/GDTGuardiaCivil.

244. Brigada de Investigación Tecnológica - Facebook. [En línea] [Citado el: 10 de enero de 2014.] https://es-es.facebook.com/BrigadaInvestigacionTecnologica.

245. Policía Nacional - Facebook. [En línea] [Citado el: 10 de enero de 2014.] https://es-es.facebook.com/PoliciaNacional.

246. Policía Nacional - Twitter. [En línea] [Citado el: 10 de enero de 2014.] https://twitter.com/Policianacional.

247. **elperiodico.com.** La cuenta de Twitter de @policia se convierte en un referente de seguridad ciudadana. [En línea] 20 de febrero de 2014. [Citado el: 3 de marzo de 2014.] http://www.elperiodico.com/es/noticias/social-media-week/cuenta-policia-convierte-referente-seguridad-ciudadana-3118110.

248. CERT-EU. [En línea] [Citado el: 3 de enero de 2014.] http://cert.europa.eu/cert/plainedition/en/cert_about.html.

249. Kenya and ITU sign administrative agreement for KE-CIRT/CC . [En línea] 17 de febrero de 2012. [Citado el: 3 de enero de 2014.] http://www.cck.go.ke/news/2012/KE-CIRT_signing.html.

250. Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC). [En línea] [Citado el: 3 de enero de 2014.] http://www.cck.go.ke/industry/information_security/ke-cirt-cc/index.html.

251. FIRST. [En línea] [Citado el: 3 de enero de 2013.] http://www.first.org/.

252. APCERT. [En línea] [Citado el: 3 de enero de 2014.] http://www.apcert.org/.

253. European Government CERTs group. [En línea] [Citado el: 4 de enero de 2014.] http://www.egc-group.org/.

254. **Consejo de Europa.** RECOMMENDATION No. R (95) 13 . [En línea] 11 de septiembre de 1995. [Citado el: 31 de diciembre de 2013.] http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec%281995%29013_en.asp.

255. —. Recommendation No. R (81) 20. [En línea] 11 de diciembre de 1981. [Citado el: 31 de diciembre de 2013.] https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=600958&SecMode=1&DocId=674076&Usage=2.

256. —. Recommendation No. R (85) 10. [En línea] 28 de junio de 1985. [Citado el: 31 de diciembre de 2013.] http://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Rec_1985_10.pdf.

257. —. Recommendation No. R (87) 15. [En línea] 17 de septiembre de 1987. [Citado el: 31 de diciembre de 2013.] http://www.un.org/en/sc/ctc/specialmeetings/2011/docs/coe/coe-rec-personaldata.pdf.

258. —. Recommendation No. R (89) 9. [En línea] 13 de septiembre de 1989. [Citado el: 31 de diciembre de 2013.] https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

259. **BOE.** Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. [En línea] 17 de septiembre de 2010. [Citado el: 30 de diciembre de 2013.] http://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

260. **ITU.** Toolkit for Cybercrime Legislation. [En línea] 2009. [Citado el: 16 de enero de 2014.] http://www.ictparliament.org/node/2130.

261. —. Toolkit for Cybercrime legislation. [En línea] febrero de 2010. [Citado el: 16 de enero de 2014.] http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf.

262. —. Cybercrimes/e-Crimes: Model Policy Guidelines & Legislative Texts. [En línea] 2012. [Citado el: 16 de enero de 2014.] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf.

263. —. Electronic Crimes: Knowledge-based Report. [En línea] 2013. [Citado el: 16 de enero de 2014.] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/ICB4PAC%20Assessment%20Eletronic%20Crime.pdf.

264. **UNODC-ITU.** Cybercrime - The global challenge. [En línea] mayo de 2011. [Citado el: 16 de enero de 2014.] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

265. **BOE.** Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [En línea] 24 de noviembre de 1995. [Citado el: 30 de diciembre de 2013.] https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

266. —. Real Decreto 1735/2010, de 23 de diciembre, por el que se establece la plantilla orgánica del Ministerio Fiscal para el año 2010. [En línea] 28 de diciembre de 2010. [Citado el: 30 de diciembre de 2013.] http://www.boe.es/boe/dias/2010/12/28/pdfs/BOE-A-2010-19954.pdf.

267. **Ministerio fiscal.** Funciones: Criminalidad informática. [En línea] 2011. [Citado el: 1 de marzo de 2014.] http://www.fiscal.es/Fiscal-especialista/Criminalidad-inform%C3%A1tica/Funciones.html?cid=1240559967849&pagename=PFiscal/Page/FGE_contenidoFinal.

268. **Irujo, José María.** El País. [En línea] 31 de octubre de 2005. [Citado el: 24 de noviembre de 2013.] http://elpais.com/diario/2005/10/31/espana/1130713201_850215.html.

269. **Belousov, Andrey.** http://www.crime-research.org/. [En línea] 19 de febrero de 2004. [Citado el: 24 de noviembre de 2013.] http://www.crime-research.org/news/19.02.2004/49/.

270. The Information Society Policy Guidelines for the Association of Finnish Local and Regional Authorities. [En línea] 2008. [Citado el: 30 de diciembre de 2013.] http://www.localfinland.fi/en/authorities/information-society/policy/Documents/AFLRA%202008%20IS%20Policy%20Guidelines.pdf.

271. Trademarks and Service Marks. [En línea] [Citado el: 3 de enero de 2014.] http://www.sei.cmu.edu/legal/marks/index.cfm.

272. TITLE 42—THE PUBLIC HEALTH AND WELFARE. [En línea] 26 de octubre de 2001. [Citado el: 29 de noviembre de 2013.] http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf.

ANEXO I: Tabla de estrategias de seguridad y documentos relacionados

Año	País	Seguridad Nacional	Seguridad información	Ciber-seguridad	Defensa	Nombre de la directiva o publicación
2000	Rusia	X				National security concept of the Russian Federation
2000	Rusia		X			Information Security Doctrine of the Russian Federation
2001	Consejo de Europa			X		Convenio sobre la ciberdelincuencia (Convenio de Budapest)
2001	ONU			X		Lucha contra la utilización de la tecnología de la información con fines delictivos
2001	Unión Europea		X			Seguridad de las redes y de la información: propuesta para un enfoque político europeo
2002	APEC			X		APEC cybersecurity strategy (propuesta del Foro de cooperación económica Asia-Pacífico)
2003	E.E.U.U.			X		The national strategy to secure cyberspace
2003	Noruega		X			National strategy for information security
2003	Reino Unido		X			Estrategia Nacional de Seguridad de la Información
2003	OEA			X		Estrategia Interamericana Integral De Seguridad Cibernética
2003	Unión Europea	X				Estrategia europea de seguridad: una Europa segura en un mundo mejor
2004	Estonia	X				National security concept of Estonia
2005	Estonia				X	National Military Strategy
2006	Japón		X			The First National Strategy on Information Security - Toward the realization of a trustworthy society
2006	Malasia			X		The National Cyber-Security Policy
2006	Suecia		X			Strategy to improve Internet security in Sweden
2007	Noruega		X			National Guidelines on Information Security 2007-2010
2007	Polonia	X				NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF POLAND
2007	Reino Unido		X			Estrategia Nacional de Seguridad de la Información
2007	UIT			X		Guía de ciberseguridad para los países en desarrollo
2007	Unión Europea			X		Hacia una política general de lucha contra la ciberdelincuencia
2008	E.E.U.U.			X		Comprehensive National Cybersecurity Initiative
2008	Eslovaquia		X			National strategy for information security in the Slovak Republic
2008	Estonia			X		Cyber Security Strategy
2008	Francia				X	The French white paper on defence and national security

Año	País	Seguridad Nacional	Seguridad información	Ciber-seguridad	Defensa	Nombre de la directiva o publicación
2008	Polonia					The Strategy for the Development of the Information Society in Poland until 2013
2008	Reino Unido	X				Estrategia de Seguridad Nacional
2009	Australia			X		Cyber Security Strategy
2009	E.E.U.U.			X		Cyberspace policy review
2009	Japón		X			The Second National Strategy on Information Security - Aiming for Strong "Individual" and “Society” in IT Age
2009	Reino Unido	X				Estrategia Nacional de Seguridad
2009	Reino Unido			X		Cyber security strategy of the United Kingdom - safety, security and resilience in cyber space
2009	UIT			X		El ciberdelito: guía para los países en desarrollo
2010	Canadá			X		Canada’s Cyber Security Strategy. For a stronger and more prosperous Canada
2010	E.E.U.U.	X				National Security Strategy
2010	Estonia	X				National security concept of Estonia
2010	Finlandia		X			Security Strategy for Society
2010	Japón		X			Information Security Strategy for Protecting the Nation
2010	Polonia			X		Governmental Program for the Protection of Cyberspace in Poland for 2011-2016
2010	Reino Unido	X				Estrategia Nacional de Seguridad
2010	República de Letonia		X			Law On the Security of Information Technologies
2010	Unión Europea	X				Estrategia de seguridad interior: Hacia un modelo europeo de seguridad
2011	Alemania			X		Cyber Security Strategy for Germany
2011	Colombia			X	X	Lineamiento de política para ciberseguridad y ciberdefensa
2011	Corea			X		National Cyber Security Masterplan
2011	E.E.U.U.			X		International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World
2011	E.E.U.U.					Cybersecurity, innovation and the internet economy
2011	E.E.U.U.			X	X	Department of Defense Strategy for Operating in Cyberspace
2011	E.E.U.U.			X		Blueprint for a Secure Cyber Future - The Cybersecurity Strategy for the Homeland Security Enterprise
2011	España	X				Estrategia Española De Seguridad
2011	Estonia				X	National Defence Strategy
2011	Francia		X			Défense et sécurité des systèmes d’information-Stratégie de la France
2011	India			X		National Cyber Security Policy
2011	Lituania			X		Programme for the Development of Electronic Information Security for 2011–2019

Año	País	Seguridad Nacional	Seguridad información	Ciber-seguridad	Defensa	Nombre de la directiva o publicación
2011	Luxemburgo			X		Stratégie nationale en matière de cyber sécurité
2011	Nueva Zelanda			X		New Zealand's Cyber Security Strategy
2011	Países Bajos			X		The National Cyber Security Strategy (NCSS) - Strength through cooperation
2011	Reino Unido			X		The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world
2011	República Checa			X		Strategy Of The Czech Republic In The Field Of Cybernetic Security For 2012 - 2015
2011	Rusia		X		X	Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space
2011	Uganda		X			National Information Security Strategy
2012	Hungría	X				Hungary's National Security Strategy
2012	Japón				X	Toward Stable and Effective Use of Cyberspace
2012	Noruega			X		Cyber Security Strategy for Norway
2012	Países Bajos			X	X	Defence Cyber Strategy
2012	Sudáfrica			X		Cyber Security policy of South Africa
2012	Suiza			X		National strategy for Switzerland's protection against cyber risks
2013	Australia				X	Defence White Paper
2013	Australia	X				Strong and Secure. A Strategy for Australia's National Security
2013	Austria			X		Austrian Cyber Security Strategy
2013	España	X				Estrategia Nacional De Seguridad
2013	España			X		Estrategia De Ciberseguridad Nacional
2013	Finlandia			X		Finland's Cyber Security Strategy
2013	Francia				X	Livre blanc défense et sécurité nationale
2013	Hungría			X		National Cyber Security Strategy of Hungary
2013	Hungría		X			Act on the Electronic Information Security of Central and Local Government Agencies
2013	Italia			X		Decree on National Cyber Security
2013	Japón			X		Cybersecurity Strategy - Toward a World-Leading, Resilient and Vigorous Cyberspace
2013	Japón			X		International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity -
2013	Países Bajos			X		National Cyber Security Strategy 2: From awareness to capability
2013	República Checa			X		Draft Act on Cyber Security
2013	Rumanía			X		Strategia De Securitate Cibernetica A Romaniei
2013	Rusia		X			Basic Principles for State Policy of the Russian Federation in the field of International Information Security
2013	Turquía	X		X	X	National Cyber Security Strategy and 2013-2014 Action Plan

Año	País	Seguridad Nacional	Seguridad información	Ciber-seguridad	Defensa	Nombre de la directiva o publicación
2013	Unión Europea		X			Proposal for a directive concerning measures to ensure a high common level of network and information security across the Union
2013	Unión Europea			X		Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

Nota: dentro de cada año, el orden en el que aparecen los distintos documentos corresponde al alfabético del nombre del país u organización.